

CYBERWORLD AND SCHOOL POLICY

NYSSBA Convention

Friday, 8:45 – 10:00 Conference Room L

October 2009

Workshop Outline

Presented by: Linda Bakst, NYSSBA Deputy Director of Policy Services, Jessica Goldstein, NYSSBA Senior Policy Consultant and Courtney Sanik, NYSSBA Policy Consultant

- I. Introduction: Putting “cyberworld” in context
 - a. For students and staff
 - b. Research findings

- II. A Skating Tour of “Cyberworld” - Demonstration
 - a. Definitions
 - b. Social Networking
 - c. Gaming
 - d. Video
 - e. Other – Twitter, Digg, Tumblr

- III. Interactive Discussion of Policy Implications for Schools
 - a. Free speech
 - b. Integrity – cheating, plagiarism
 - c. Search and seizure
 - d. Bullying/harassment
 - e. Privacy

- IV. The Policy Response
 - a. Brief review of policies a district should have
 - b. Review of Computer Resources and Data Management (8630)
 - c. Review of Internet Safety (4526.1)

- V. Summary and Q & A: Where do we go from here?

INTERNET SAFETY

NOTE: This has been a required policy under federal law since 2001, which NYSSBA has updated recently due to a change in federal law. Under the Broadband Data Services Improvement Act/Protecting Children in the 21st Century Act of 2008 (P.L. 110-385), school districts and BOCES must now, as part of their Internet Safety Policy (which is required in order to receive E-Rate discounts), educate minors about appropriate online behavior, including:

- *Interacting with other individuals on social networking sites and in chat rooms; and*
- *Cyberbullying awareness and response.*

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 computer network coordinator 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 regulation. He or she also shall be responsible for ensuring that staff and students receive training on their requirements.

NYSSBA Sample Policy 4526.1

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.

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.

NOTE: Your district may already cover appropriate online behavior in its "Acceptable Use" policy for use of district computers and the internet. If so, we would recommend that the Board review that Acceptable Use policy as well, (the NYSSBA policy number is 4526) to make sure that it is in accordance with the new requirements.

Your district may also already provide instruction on bullying prevention, including cyberbullying which includes awareness and response. If that is the case, you can modify our suggested text to reflect district practice.

Cross-ref: 4526, Computer Use in Instruction

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
47 USC §254
20 USC §6777

Adoption date:

INTERNET SAFETY REGULATION

NOTE: We have revised our template regulation by adding the bold text below (see section IV, Training) to comply with new legal requirements for the E-Rate discounts.

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 or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves 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 a 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.

NYSSBA Sample Regulation 4526.1-R

- The district's computer network coordinator shall be responsible for ensuring the installation and proper use of any Internet blocking and filtering technology protection measure obtained by the district.
- The computer network coordinator 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 computer network coordinator 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 computer network coordinator 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.
- Except as otherwise authorized under the district's Computer Network or Acceptable Use Policy, students may use the district's computer network to access the Internet and World Wide Web only during supervised class time, study periods or at the school library, and exclusively for research related to their course work.
- 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 computer network coordinator 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 computer network coordinator 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.

NYSSBA Sample Regulation 4526.1-R

- 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.

NOTE: We have added the bold text in the bullet below to implement the new curricular provision of federal law relating to internet safety policies, as noted above.

- **The district shall provide age-appropriate instruction to students regarding appropriate online behavior. Such instruction 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 how to recognize and respond to cyberbullying 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.
- The Principal 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 teachers.

Adoption date:

COMPUTER RESOURCES AND DATA MANAGEMENT

NOTE: This is not a required policy, but the appropriate management of computer resources and electronic data has become increasingly important. It has also become a focus of attention for auditors. We offer this policy as a tool to address these issues. In addition, if a district's acceptable computer use policy is only for students and doesn't cover employees, this policy could serve that purpose as well.

The Board of Education recognizes that computers are a powerful and valuable education and research tool and as such are an important part of the instructional program. In addition, the district depends upon computers as an integral part of administering and managing the schools' resources, including the compilation of data and recordkeeping for personnel, students, finances, supplies and materials. This policy outlines the Boards expectations in regard to these different aspects of the district's computer resources.

General Provisions

The Superintendent shall be responsible for designating a **[computer network coordinator – insert appropriate title]** who will oversee the use of district computer resources. The **[insert title]** will prepare in-service programs for the training and development of district staff in computer skills, appropriate use of computers and for the incorporation of computer use in subject areas.

NOTE: The district may distinguish responsibility for integrating computers into instruction from use of computers in district operations by assigning these tasks to different individuals. If that is indeed the practice of the district, please insert language that reflects that division of responsibility here.

The Superintendent, working in conjunction with the designated purchasing agent for the district, and **[insert other appropriate personnel who would be involved in determining instructional computer needs]**, will be responsible for the purchase and distribution of computer software and hardware throughout the 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.

The Superintendent, working with the **[insert title]**, shall establish regulations governing the use and security of the district's computer resources. The security and integrity of the district computer network and data is a serious concern to the Board and the district will make every reasonable effort to maintain the security of the system. All users of the district's computer resources shall comply with this policy and regulation, as well as the district's **[insert name of district's computer acceptable use policy]**(4526). Failure to comply may result in disciplinary action, as well as suspension and/or revocation of computer access privileges.

NYSSBA Sample Policy 8630

All users of the district's computer resources must understand that use is a privilege, not a right, and that use entails responsibility. Users of the district's computer network must not expect, nor does the district guarantee, privacy for electronic mail (e-mail) or any use of the district's computer network. The district reserves the right to access and view any material stored on district equipment or any material used in conjunction with the district's computer network.

Management of Computer Records

The Board recognizes that since district data is managed by computer, it is critical to exercise appropriate control over computer records, including financial, personnel and student information. The Superintendent, working with the **[insert title]** and the district's business official, shall establish procedures governing management of computer records. The procedures will address:

- passwords,
- system administration,
- separation of duties,
- remote access,
- data back-up (including archiving of e-mail),
- record retention, and
- disaster recovery plans.

Review and Dissemination

Since computer technology is a rapidly changing area, it is important that this policy be reviewed periodically by the Board and the district's internal and external auditors. The regulation governing appropriate computer use will be distributed annually to staff and students and will be included in both employee and student handbooks.

Cross-ref: 1120, School District Records
 4526, Computer Use for Instruction
 4526.1, Internet Safety
 6600, Fiscal Accounting and Reporting
 6700, Purchasing
 8635, Information Security Breach and Notification

Adoption date:

COMPUTER RESOURCES AND DATA MANAGEMENT REGULATION

The following rules and regulations govern the use of the district's computer network system, employee access to the Internet, and management of computerized records.

I. Administration

- 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 system.
- The computer network coordinator shall develop and implement procedures for data back-up and storage. These procedures will facilitate the disaster recovery plan and will comply with the requirements for records retention in compliance with the district's policy on School District Records (1120).
- The computer network coordinator 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 computer network coordinator 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 (including policy 4526, Computer Use in Instruction) governing use of the district's network.
- The computer network coordinator shall take reasonable steps to protect the network from viruses or other software that would comprise the network.
- All student and employee agreements to abide by district policy and regulations and parental consent forms shall be kept on file in the district office.
- Consistent with applicable internal controls, the Superintendent in conjunction with the school business official and the computer network coordinator, will ensure the proper segregation of duties in assigning responsibilities for computer resources and data management.

II. Internet Access

Student Internet access is addressed in policy and regulation 4526, Computer Use for Instruction. District employees and third party users are governed by the following regulations:

[Note: The School Board should amend these access provisions as appropriate]

- Employees will be issued an e-mail account through the district's computer network.
- Employees are expected to review their e-mail daily.
- Communications with parents and/or students should be saved and the district will archive the e-mail records according to procedures developed by the computer network coordinator.

NYSSBA Sample Regulation 8630-R

- Employees may access the internet for education-related and/or work-related activities.
- Employees shall refrain from using computer resources for personal use.
- Employees are advised that they must not have an expectation of privacy in the use of the district's computers.
- Use of computer resources in ways that violate the acceptable use and conduct regulation, outlined below, will be subject to discipline.

III. Acceptable Use and Conduct

The following regulations apply to **all staff and third party users** of the district's computer system:

- Access to the district's computer network is provided solely for educational and/or research purposes and management of district operations 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.
- 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 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 language, vulgarities and swear words are all inappropriate.
- Network users identifying a security problem on the district's network must notify appropriate staff. 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 for **all staff and third party users** concerning use of the district's computer network. Any violation of these prohibitions may result in discipline or other appropriate penalty, including suspension or revocation of a user's access to the network.

- 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.

NYSSBA Sample Regulation 8630-R

- Using the network to receive, transmit or make available to others messages that are racist, sexist, abusive or harassing to others.
- Use of another's account or password.
- Attempting to read, delete, copy or modify the electronic mail (e-mail) of other system users.
- 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.
- 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.
- 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 fraudulent purposes or financial gain.
- Stealing data, equipment or intellectual property.
- Gaining or seeking to gain unauthorized access to any files, resources, or computer or phone systems, or vandalize 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 your 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.

V. No Privacy Guarantee

Users of the district's computer network should not expect, nor does the district guarantee, privacy for electronic mail (e-mail) or any use of the district's computer network. The district reserves the right to access and view any material stored on district equipment or any material used in conjunction with the district's computer network.

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 disciplinary action as well as suspension and/or revocation of computer access privileges.

NYSSBA Sample Regulation 8630-R

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.

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, misdeliveries, or service interruptions caused by its own negligence or any other errors or omissions. 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 regulation.

Adoption date: