NYSSBA Sample Policy 8630

( ) Required
(X) Local
( ) Notice

COMPUTER RESOURCES AND DATA MANAGEMENT

NEW NOTE: We have included language to address school district audits by the Office of State Comptroller regarding security of district information on computer resources.

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.

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.

OLD NOTE: In view of increasing concern about the vulnerability of computer systems to unauthorized access to personally identifiable data, NYSSBA recommends making the paragraph that follows more comprehensive by recognizing that fax machines and copiers need to be considered as part of the district's approach to data security.

The Superintendent, working with the **[insert title]**, shall establish regulations governing the use and security of the district's computer resources (computer resources include all devices that process data, including but not limited to, laptops, fax machines, copiers and scanners). 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 policy 4526, Computer Use in Instruction. Failure to comply may result in disciplinary action, as well as suspension and/or revocation of computer access privileges.

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

OLD NOTE: If the district is utilizing offsite or "cloud" storage, be aware that local, state and federal privacy and access provisions still apply and should be addressed by the company/contractor. Regardless of the location of the server storing the district's records, the district needs to be sure that they can abide by all United States and New York State laws and regulations regarding record access and retention. Language to address this is offered below. The sixth, seventh, and eighth bullets below address protection of district computer resources and information, including disposal of district computer resources and equipment inventory:

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 **[If the district is utilizing Cloud Computing, then the following language should be considered**: taking into account whether the records are stored onsite on district servers or on remote servers in the "cloud"]. The procedures will address:

- passwords,
- system administration,
- separation of duties,
- remote access,
- encryption,
- user access and permissions appropriate to job titles and duties,
- disposal of computer equipment and resources (including deleting district data or destroying the equipment),
- inventory of computer resources (including hardware and software),
- data back-up (including archiving of e-mail),
- record retention, and
- disaster recovery plans and notification plans.

If the district contracts with a third-party vendor for computing services, the Superintendent, in consultation with ***[insert applicable titles, such as Director of Technology, Business Official, School Attorney],*** will ensure that all agreements address the procedures listed above, as applicable.

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
5500, Student Records
6600, Fiscal Accounting and Reporting
6700, Purchasing
6900, Disposal of District Property
8635, Information Security Breach and Notification

Adoption date:

NYSSBA Sample Regulation 8630-R

COMPUTER RESOURCES AND DATA MANAGEMENT REGULATION

NEW NOTE: This regulation includes language to address school district audits by the Office of State Comptroller regarding security of district information on computer resources (see second bullet under section I. below). Districts are encouraged to review their current policies, regulation and procedures to make sure that they are taking the necessary precautions to ensure data security.

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 work with the [**insert district individual in charge of maintaining inventory**] to maintain an updated inventory of all computer hardware and software resources.
- The computer network coordinator shall develop and implement procedures for data back-up and storage. These procedures will facilitate the disaster recovery and notification plan and will comply with the requirements for records retention in compliance with the district's policy on School District Records (1120). **[If the district is utilizing Cloud Computing, then the following language should be considered to be added to the previous sentence:** taking into account the use of onsite storage or storage in the cloud].
- 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, other software, and network security risks that would compromise the network or district information.
- 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 in Instruction. District employees and third party users are governed by the following regulations:

OLD 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 as appropriate and the district will archive the e-mail records according to procedures developed by the computer network coordinator.
- 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:

NEW NOTE: The fourth and sixth bullets below address some human causes for computer security breaches.

- 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 and must be of sufficient complexity as determined by the district.
- 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 take reasonable precaution to secure district information stored on devices they use, including maintaining responsible custody over computer resources, ensuring no unauthorized use of district devices, and exercising prudent judgement when browsing the internet and opening email.

- 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.

NOTE: The last bullet below addresses some human causes for computer security breaches.

- 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.
- 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, malware on the network, and not reporting security risks as appropriate.
- 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, using personal disks, or downloading files 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.
- Exhibiting careless behavior with regard to information security (e.g., sharing or displaying passwords, leaving computer equipment unsecured or unattended, etc.).

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.

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 the user's 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.

NOTE: The paragraph below includes language to address protection of district computer resources and information with regard to disposal of district computer resources.

The district will take reasonable steps to protect the information on the network and provide a secure network for data storage and use, including ensuring that contracts with vendors address data security issues and that district officials provide appropriate oversight. Disposal of district computer resources shall ensure the complete removal of district information, or the secure destruction of the resource. Even though the district may use technical and/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: