Business/Non-Instructional Operations

Computer Security

The Board of Education desires/believes that direction, procedures, requirements and responsibilities be established, delineated and maintained to ensure the appropriate protection and security of the District's computers, networked or stand-alone.

The Superintendent of Schools is directed to establish guidelines and procedures to protect and ensure the security of all District computers, telecommunication equipment and information handled by such equipment.

(cf. 3523.1 - Acquisition and Updating of Technology)
(cf. 4118.4/4218.4 - Electronic Mail)
(cf. 6141.32 - Technology and Instruction)
(cf. 6141.321 - Acceptable Use of the Internet)
(cf. 6141.322 - WebSites/Pages)
(cf. 6156 - Use of Computers in Instruction)
(cf. 6161.7 - Use of Proprietary Software Products)
(cf. 6162.6 - Copyright)
(cf. 6162.7 - Educational Software)
(cf. 9327 - Electronic Mail Communications)

Legal Reference: Connecticut General Statutes

The Freedom of Information Act

PA 98-142 An Act Requiring Notice to Employees of Electronic Monitoring by Employers

Public Law 94-553, The Copyright Act of 1976, U.S.C. 101 et. seq.

Policy adopted: August 25, 2003

NEW HAVEN PUBLIC SCHOOLS
New Haven, Connecticut

Business/Non-Instructional Operations

Computer Security

Purpose

The purpose of this regulation is to establish direction, procedures, requirements, and responsibilities to ensure the appropriate protection of the New Haven Public Schools computer and telecommunication equipment and information handled by computers, networked or standalone.

Scope

This regulation applies to all full-time, part-time, and intermittent District employees to include grant-funded position employees. This regulation also applies to contractors, consultants, temporaries, interns, elected officials and others at the New Haven_ Public Schools, including those Users affiliated with third parties who access the New Haven_ Public Schools computer systems. Throughout this regulation, the word "User" will be used to collectively refer to all such individuals. The regulation also applies to all computer and data communication systems (telecommunication systems) used at, owned by and/or administered by the New Haven_ Public Schools, whether the systems are standalone or connected to a network such as LAN or WAN, the Internet or the Intranet.

Responsibilities

The Technology Coordinator of the New Haven Public Schools is responsible for establishing, maintaining, implementing, administering, and interpreting organization-wide information systems security policies, standards, guidelines, and procedures. While responsibility for information system's security on a day-to-day basis is every user's duty, specific guidance, direction, and authority for information systems security is centralized for all of the District Public Schools. He/she may perform information system risk assessments, prepare information systems security action plans, evaluate information security products, and perform other activities necessary to assure a secure information systems environment.

The Technology Coordinator and the Business Manager share responsibility for conducting or coordinating investigations into any alleged computer or network security compromises, incidents, or problems. All security compromises or potential security compromises must be reported to the Technology Coordinator.

Business/Non-Instructional Operations

Computer Security

Responsibilities (continued)

Administrators are responsible for ensuring that appropriate computer and telecommunication system security measures are observed in their buildings and departments. Administrators are responsible for making sure that all Users in their department are aware of the New Haven_ Public Schools' policies and regulations related to computer and telecommunications systems security and use. They are also responsible for reporting all suspicious computer and network security-related activities and/or any known violations of this regulation to the Technology Coordinator. They are responsible for administering appropriate disciplinary actions. They also serve as local information security liaisons, implementing and keeping informed of the requirements of this and other information systems security policies, standards, guidelines, and procedures.

User Responsibilities

Users are responsible for complying with all New Haven Public Schools policies and regulations defining computer and network security measures and use.

Audit Compliance

From time to time, the Technology Coordinator may designate individuals to audit compliance with computer and network security policies. At the same time, every User must promptly report any suspected network security problem, including intrusions and out-of-compliance situations, to the Technology Coordinator.

Tools to Compromise Systems Security

Unless specifically authorized by the Technology Coordinator, New Haven Public Schools Users must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security. Examples of such tools include those that defeat software copy-protection, discover secret passwords, identify security vulnerabilities, or decrypt encrypted files. Unless specific permission has been obtained from the Technology Coordinator, Users are prohibited from using such tools.

Requests from outside entities that the New Haven Public Schools security mechanisms be compromised must NOT be satisfied unless approved in advance by the Technology Coordinator or the Business Manager or the New Haven Public Schools is compelled to comply by law. Likewise, short cuts bypassing systems security measures, as well as pranks and practical jokes involving the compromise of systems security measures are absolutely prohibited.

Business/Non-Instructional Operations

Computer Security (continued)

Reporting Problems

All network or systems software malfunctions, including information security alerts, warnings, suspected vulnerabilities and the like, must be immediately reported to the Technology Coordinator. Ignoring these malfunctions could lead to serious problems such as lost or damaged information as well as unavailable network services.

Users are prohibited from using New Haven Public Schools systems to forward such malfunction or security information to another User, whether the other User is internal or external to the New Haven Public Schools.

Screen Savers

Windows systems provide an approved screen saver. All other screen savers must be pre-approved by the Technology Coordinator. It is recommended that a screen saver be used if sensitive information resides on a microcomputer. In that way, whenever a worker leaves their desk, the screen should be immediately obscured by setting the screen saver to be activated after a period of no activity or shutting down the computer.

Individual Departmental Regulations

Department specific rules regarding microcomputers must comply with this and all other New Haven Public Schools security policies and regulations. Individual department rules could exceed, but not be less than the guidelines covered in all security regulations.

Exceptions

The Technology Coordinator acknowledges that under rare circumstances, certain Users will need to employ systems that are not compliant with these regulations. ALL such instances must be approved in writing and in advance by the Coordinator of Technology.

Violations

The New Haven Public Schools User who willingly and deliberately violates this regulation will be subject to disciplinary action up to and including termination, as defined by the appropriate contract. Further, those whose conduct not only violates this regulation but also violate other District work rules may also receive such additional disciplinary action as would otherwise be undertaken (which may include suspension from duty without pay or discharge). Should a violation of this regulation also constitute an act prohibited by law, appropriate law enforcement officials may be contacted.

Business/Non-Instructional Operations

Computer Security (continued)

Remote Printing

Printers must not be left unattended if "restricted" or "confidential" (closed records) information is being printed or will soon be printed. The persons attending the printer must be authorized to examine the information being printed. Unattended printing is permitted if the area surrounding the printer is physically protected such that persons who are not authorized to see the material being printed may not enter.

Access Paths and Configuration Control

Network Changes

Changes to the New Haven_ Public Schools internal networks include loading new software, changing network addresses, reconfiguring routers, adding dial-up lines, etc. With the exception of emergency situations, all changes to the New Haven_ Public Schools computer networks must be: (a) documented in a service request, and (b) approved in advance by the Technology Coordinator except as explicitly delegated by him/her. Emergency changes to the New Haven_ Public Schools networks must only be made by persons who are authorized by the Technology Coordinator or the Business Manager. This process prevents unexpected changes from inadvertently leading to denial of service, unauthorized disclosure of information, waste of resources, and other problems.

New Date Lines

Users must not arrange for, or actually complete the installation of data lines with any carrier, without first discussing in detail the plans with the Business Manager.

Miscellaneous Connections

Users must NOT establish electronic bulletin boards, local area networks, modem connections to existing local area networks, or other multi-user systems for communicating information without the specific approval of the Technology Coordinator.

New types of real-time connections between two or more in-house computer systems or connecting computers to existing networks must not be established unless such approval has first been obtained. This regulation helps to ensure that all the New Haven_ Public Schools systems have the controls needed to protect other network-connected systems. Security requirements for a network-connected system are not just a function of the connected system; they are also a function of all other New Haven_ Public Schools connected systems.

Business/Non-Instructional Operations

Computer Security (continued)

Providing Network Services To Third Parties

Participation in external networks as a provider of services that external parties rely on is expressly prohibited unless the following conditions are fulfilled. (1) the New Haven_ Public Schools legal counsel must identify the legal risks involved, (2) the Technology Coordinator recommends these and other risks associated with the proposal, (3) Business Manager approval.

Changes to Application Software

The New Haven_ Public Schools has a standard list of permissible software packages that users can run on their microcomputers. Users must not install other software packages on their computers without obtaining advance permission from the Technology Coordinator. Users must not permit automatic software installation routines to be run without prior approval. Autodiscovery license management software could be used by the Technology Coordinator to remotely determine which software packages are resident on User hard disks; unapproved software may be removed without User advance notice.

Changes To Operating System Configurations

On District owned computers, Users must not change operating system configurations, upgrade existing operating systems, or install new operating systems. If such changes are required, they will be performed by recommendation from the Technology Coordinator.

Changes To Hardware

Computer equipment supplied by the New Haven_ Public Schools must not be altered or added to in any way (e.g. upgraded processor, expanded memory, or extra circuit boards) without recommendation from the Technology Coordinator and approval by the Business Manager.

Remote Maintenance and Outbound Dial-Up Connections

Remote maintenance ports for the New Haven_ Public Schools computer and telecommunication systems might be disabled until the specific time as they are needed by the vendor. These ports must then be again disabled immediately after use. Alternatively, dial-up connections can be established with vendors via outbound calls initiated by New Haven_ Public Schools' User.

Business/Non-Instructional Operations

Computer Security (continued)

Passwords

Passwords Are Required

The purpose of passwords is to protect the __ New Haven Public Schools and direct access to the various programs utilized by Users in the District.

All Users using computers that are permanently or intermittently connected to the New Haven Public Schools networks must have password access controls. Computer and telecommunication system access control must be achieved via passwords which are unique to each individual User. Multi-user systems must employ User-Ids and passwords unique to each User, as well as User privilege restriction mechanisms.

Password Assignment

All Users will be issued a password by the school department in order to start up all of their computers and to access the network. Passwords will be changed periodically as part of normal security maintenance. Using passwords that have not been assigned by the school department is prohibited without prior notification and identification to the Technology Coordinator.

Shared Passwords Prohibited

Access controls to files, applications, databases, computers, networks, and other system resources via shared passwords (also called "group passwords") is prohibited.

Storing And Disclosure Of Passwords

Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, in computers without access control, posted to walls, or in other locations where unauthorized persons might discover them.

Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the authorized User. To do so exposes the authorized User to responsibility for actions that the other party takes with the disclosed password. If Users need to share computer resident data, they should use electronic mail, public directories on local area network servers, or other mechanisms. This regulation does not prevent use of default passwords, typically used for new User-ID assignment, password reset situations, or are vendor-supplied, which must immediately be changed when the User next logs onto the involved system.

Passwords must be immediately changed if they are suspected of being disclosed, or known to have been disclosed to anyone besides the authorized User.

Business/Non-Instructional Operations

Computer Security (continued)

Compromised System Security

Whenever system security has been compromised, or even if there is a convincing reason to believe that it has been compromised, the school department will reassign all relevant passwords and force every password on the involved system to be changed at the time of the next log-in. If systems software does not provide the latter capability, all Users will be informed that they must change their passwords immediately.

Computer and Network Use

Recognizing that the New Haven Public Schools computer and network and telecommunications systems are owned by same, Users must use this property for business purposes only.

Town Access

The New Haven Public Schools reserves the right to access stored records. Users should not expect that files stored on District servers are private. Network supervision and maintenance may require review and inspection of directories, files, and/or e-mail messages to maintain system integrity and security and assure proper use.

Communications Over Network

Because communications over the network are often public in nature, it is important the User realize that privacy in communications may not be guaranteed. Messages may accidentally be diverted to a destination other than the one intended. Therefore, caution should be exercised when sharing/transmitting any information because messages may not be entirely secure. Further, the dissemination of information/records should be consistent with municipal, state and federal laws, as well as, general rules and standards regulating privacy and fair information practices.

Personal Use

The _ New Haven Public Schools allows for incidental personal use of its computer and network and telecommunication systems if the use:

a. does not consume more than a trivial amount of resources that could otherwise be used for business purposes,
b. does not interfere with User productivity,
c. does not preempt any District-business activity,
d. is not for communicating financial information without the proper authorization,

Business/Non-Instructional Operations

Computer Security

Personal Use (continued)

e. is not for any purposes that will produce personal financial gains,
f. is not for distribution or printing of copyrighted materials (including articles and software) violating copyright laws,
g. is not for violating any regulations, etc., prescribed by a software and/or network provider,
h. is not for sending, receiving, printing, or otherwise distributing proprietary data or other confidential information of the New Haven_ Public Schools violating District regulation,
i. is not for creating, downloading, copying, storing, sending, voluntarily receiving or soliciting offensive, improper, defaming or harassing statements or language; including those that may create an intimidating or hostile work environment, including disparagement of others based on their race, marital status, national origin, sex, sexual orientation, age, disability, religious or political beliefs,
j. is not for accessing, sending, voluntarily receiving or soliciting sexually oriented messages or images, whose contents infer, contain, or are explicit, etc., including but not limited to, Web sites or materials,
k. is not for displaying offensive, sexually explicit, etc., messages, pictures or material,
l. is not used for sending chain letters, gambling, or engaging in any other activity which violates the law,
m. is not for assisting or running a campaign for election of any person to any office,
n. is not for promoting or opposing any ballot proposition or political issue without authorization,
o. is not for promoting supporting or celebrating religion or religious institutions,
p. is not for using and/or accessing a computer, including but not limited to, files, documents or messages, without authorization,
q. is not for intentionally damaging, erasing, or corrupting any software, folders, documents, files, etc., including but not limited to, engaging in practices that threaten the computer/network, etc., (e.g. loading files that may introduce a virus).

The above are guidelines and are not intended to be exclusive. In general, all acts that violate the spirit and intent of general rules and standards for professional conduct of behavior and of communications and dispensing of information may be considered to violate this regulation and may subject the User to disciplinary action up to and including termination. This regulation will be enforced and interpreted consistent with other employment policies like, but not limited to, anti-discrimination and sexual harassment.

Notwithstanding such disciplinary as may be contemplated, initiated or effectuated the Director of Technology reserves the right to deny a User who violates this regulation all or a portion of network and/or computer access.

Business/Non-Instructional Operations

Computer Security

(cf. 3523.1 - Acquisition and Updating of Technology)
(cf. 4118.4/4218.4 - Electronic Mail)
(cf. 6141.32 - Technology and Instruction)
(cf. 6141.321 - Acceptable Use of the Internet)
(cf. 6141.322 - WebSites/Pages)
(cf. 6156 - Use of Computers in Instruction)
(cf. 6161.7 - Use of Proprietary Software Products)
(cf. 6162.6 - Copyright)
(cf. 6162.7 - Educational Software)
(cf. 9327 - Electronic Mail Communications)

Legal Reference: Connecticut General Statutes

The Freedom of Information Act

PA 98-142 An Act Requiring Notice to Employees of Electronic Monitoring by Employers

Public Law 94-553, The Copyright Act of 1976, U.S.C. 101 et. seq.

Regulation approved: August 25, 2003

NEW HAVEN PUBLIC SCHOOLS
New Haven, Connecticut