

BOARD OF EDUCATION REGULATION

EMPLOYEE COMPUTER, NETWORK, INTERNET, AND E-MAIL USE RULES

The Board of Education is committed to the goal of having electronic network facilities used in a responsible, efficient, ethical and legal manner. Access to telecommunications (Internet and e-mail) is provided for employees to conduct research and communicate with others in relation to school business. Access to these network services is provided to employees who agree to act in a considerate and responsible manner.

Access is a privilege, not a right Therefore, based upon acceptable use guidelines outlined in this policy, network administrators and members of the Technology Committee will deem what is inappropriate use and their decisions are final. The network administrators may close a telecommunications account at any time. Users must acknowledge their understanding of this policy as a condition of using a district Internet account or using the network facilities.

Employees have no expectation of privacy when using the school's computers, networks, Internet services, e-mail and other technology. Further, employees are advised that there are inherent risks of identity theft, fraud, loss of privacy and other hazards when using technology. The school assumes no liability for any loss by an employee when using its technology.

Failure to comply with board policy and other procedures or rules governing computers, networks, Internet services, and/or e-mail may result in disciplinary action, up to and including discharge. Illegal uses of the school's computers, networks, Internet services, and/or e-mail may also result in referral to law enforcement authorities.

A. Access to School Computers, Networks, Internet Services, and E-mail

The level of access that employees have to school unit computers, networks, Internet services, and/or e-mail is based upon specific employee job requirements and needs.

B. Acceptable Use

In general, use of the computer systems, including access to the Internet is limited to school related activities. Activities such as e-mailing parents, inquiries on behalf of students, education related Web sites, the State Education Department Web site, purchasing of school related products, e-mailing of work related documents and alumni e-mails are not considered personal use.

Incidental personal use is permitted during certain times of the day. All use of the Internet and e-mail, whether school related or personal use is subject to review by the School District and members of the Technology Committee. The following activities (in addition to school related uses) are permissible before school, during lunch and after school so long as the activities do not interfere with the employee's performance or the education mission of the District:

1. Review of on-line publications/newspapers.
2. Reviewing weather, movie times, travel directions, etc.
3. E-mail correspondence.
4. Making medical appointments.
5. On-line banking or bill paying.
6. Making reservations.
7. Review of courses available for graduate work.
8. Shopping related Web sites for short durations.
9. Professional listservs.
10. Correspondence with colleagues.

In addition, e-mail to family members is permissible at anytime except during duty and class periods.

Under no circumstances will uses described in the policy as prohibited uses be permitted. Operation of private businesses by employees from school buildings (including the use of the Internet for such purposes) is prohibited.

C. Prohibited Use

The employee is responsible for his/her actions and activities involving school unit computers, networks, Internet services, and for e-mail as well as for his/her computer files, passwords, and accounts. General examples of unacceptable uses, which are expressly prohibited, include, but are not limited to the following:

1. Any use that is illegal or in violation of other board policies, including harassing, discriminatory or threatening communications and behavior; violations of copyright laws, etc.;
2. Any use involving materials that are obscene, pornographic, sexually explicit, or sexually suggestive;
3. Any inappropriate communications with students, minors, or adults;
4. Any use for private financial gain, or commercial, advertising or solicitation purposes;
5. Any use as a forum for communicating by e-mail or any other medium with other school users or outside parties to solicit, proselytize, advocate or communicate the views of an individual or non-school sponsored organization; to solicit membership in or support of any non-school sponsored organization; or to raise funds for any non-school sponsored purpose, whether profit or non-for-profit. No employee shall knowingly provide school e-mail addresses to outside parties whose intent is to communicate with school employees, students and/or their families for non-school purposes. Employees who are uncertain as to whether particular activities are acceptable should seek further guidance from the District Director of Technology;
6. Any communication that represents personal views as those of the school unit or that could be misinterpreted as such;
7. Downloading or loading software or applications; including inappropriate screen savers, unauthorized music, etc.;
8. Opening or forwarding any e-mail or e-mail attachments from unknown sources and/or that may contain viruses;
9. Sending mass e-mails to school users or outside parties for school or non-school purposes with out the permission of the District Director of Technology;
10. Any malicious use or disruption of the school unit's computers, networks, Internet services and/or e-mail or breach of security features;

11. Any misuse or damage to the school unit's computer equipment;
12. Misuse of the computer passwords or accounts (employee or other users);
13. Any communications that are in violation of generally accepted rules of network etiquette and/or professional conduct;
14. Any attempt to access unauthorized sites; unless necessary for instruction such as research on cancer, pharmaceutical drugs, etc.
15. Failing to report a known breach of computer security to the District Director of Technology;
16. Using school computers, networks, Internet services and/or e-mail after such access has been denied or revoked; and
17. Any attempt to delete, erase or otherwise conceal any information that violates these rules and that is stored on a school computer.

D. No Expectation of Privacy

The school unit retains control, custody and supervision of all computers, networks, Internet and e-mail services owned or leased by the school unit. The school unit reserves the right to monitor all computer and Internet activity by employees and other system users. Employees have no expectation of privacy in their use of school computers, including e-mail messages and stored files.

E. Confidentiality of Information

Employees are expected to use appropriate judgment and caution in communications concerning students and staff to ensure that personally identifiable information remains confidential.

F. Staff Responsibilities to Students

Teachers, staff members and volunteers who utilize school computers for instructional purposes with students have a duty of care to supervise such use. Teachers, staff members and volunteers are expected to be familiar with the school unit's policies and rules concerning student computer and Internet use and to enforce them. When in the course of their duties, employees/volunteers become aware of student violations they are expected to stop the activity and inform the building Instructional Technology Support Staff who will then inform the District Director of Technology.

G. Compensation for Losses, Costs and/or Damages

The employee shall be responsible for any losses, costs or damages incurred by the school unit related to violations of the EMPLOYEE COMPUTER, NETWORK, INTERNET, AND E-MAIL USE POLICY and/or these rules.

H. School Unit Assumes No Responsibility for Unauthorized Charges, Costs, or Illegal Use

The school unit assumes no responsibility for any unauthorized charges made by employees, including but not limited to credit card charges, subscriptions, long distance telephone charges, equipment and line costs, or for any illegal use of the computers such as copyright violations.

I. Employee Acknowledgement Required

Each employee authorized to access the school unit's computers, networks, Internet services, and/or e-mail is required to sign an acknowledgement form stating that he/she has read the EMPLOYEE COMPUTER, NETWORK, INTERNET, AND E-MAIL USE POLICY and these rules. The acknowledgement form will be retained in the employee's personnel file.

Adoption date: May 3, 2005

BOARD OF EDUCATION POLICIES

**EMPLOYEE COMPUTER, NETWORK, INTERNET, AND E-MAIL USE ACKNOWLEDGMENT
FORM**

Each employee shall sign and return this acknowledgment to indicate receipt of the Policy.

I have read the Nyack Union Free School District's EMPLOYEE COMPUTER, NETWORK, INTERNET, AND E-MAIL USE POLICY and EMPLOYEE COMPUTER, NETWORK, INTERNET, AND E-MAIL USE RULES and understand their terms and conditions.

Signature

Date

Adoption date: May 3, 2005

BOARD OF EDUCATION POLICIES

EMPLOYEE COMPUTER, NETWORK, INTERNET, AND E-MAIL USE

The Nyack Union Free School District provides computers, networks, Internet access, and/or e-mail to support the educational mission of the schools and to enhance the curriculum and learning opportunities for students and school staff.

Any employee who violates this policy and/or any rules governing use of the school unit's computers, networks, Internet services, and/or e-mail will be subject to disciplinary action, up to and including discharge. Illegal uses of the school unit's computers, networks, Internet services, and/or e-mail will also result in referral to law enforcement authorities.

Nyack Union Free School District's computers, networks, Internet services, and/or e-mail remain under the control, custody and supervision of the school unit. The school unit reserves the right to monitor all computer, network, Internet and/or e-mail activity by employees. Employees have no expectation of privacy in their use of school computers.

Each employee authorized to access the school unit's computers, networks, Internet services and/or e-mail is required to sign an acknowledgement form stating that they have read this policy and the accompanying rules. The acknowledgement form will be retained in the employee's personnel file.

The superintendent shall be responsible for overseeing the implementation of this policy and the accompanying rules, and for advising the board of the need for any future amendments or revisions to the policy/rules. The superintendent may develop additional administrative procedures/rules governing the day-to-day management and operations of the school unit's computer system as long as they are consistent with the board's policy/rules. The superintendent may delegate specific responsibilities to the District Director of Technology, building principals and others, as he/she deems appropriate.

Adoption date: May 3, 2005