

## **Personnel - Certified-Non-Certified**

### **Rights, Responsibilities and Duties**

#### **Acceptable Computer Network Use (Employee Use of Technology)**

The Board of Education recognizes that technological resources can enhance employee performance by offering effective tools to assist in providing a quality instructional program, facilitating communications with parents/guardians, students, and the community, supporting District and school operations, and improving access to and exchange of information. The Board expects all employees to learn to use the available technological resources that will assist them in the performance of their job responsibilities. As needed, employees shall receive professional development in the appropriate use of these resources.

Employees shall be responsible for the appropriate use of technology and shall use the District's technological resources primarily for purposes related to their employment.

Employees shall be notified that computer files and electronic communications, including email and voice mail, are not private. Technological resources shall not be used to transmit confidential information about students, employees, or District operations without authority.

#### **Online/Internet Services**

**Note:** 20 USC 6777 mandates that districts adopt an Internet safety policy as a condition of receiving technology funds under Title II, Part D of the No Child Left Behind Act (20 USC 6751-6777) for the purpose of purchasing computers with Internet access or paying for direct costs associated with accessing the Internet. 47 USC 254 mandates that districts adopt an Internet safety policy in order to qualify for federal universal service discounts for Internet access (E-rate discounts). Although these requirements focus on measures designed to protect students using district technology, they also require policy that affects adult use of any district computers with Internet access. Districts applying for any of these funds must certify that District policy requires the operation and enforcement of a "technology protection measure" that blocks or filters Internet access to visual depictions that are obscene or child pornography.

The Superintendent or designee shall ensure that all District computers with Internet access have a technology protection measure that prevents access to visual depictions that are obscene or child pornography and that the operation of such measures is enforced. The Superintendent or designee may disable the technology protection measure during use by an adult to enable access for bona fide research or other lawful purpose. (20 USC 6777; 47 USC 254)

## **Personnel - Certified-Non-Certified**

### **Rights, Responsibilities and Duties**

#### **Acceptable Computer Network Use (Employee Use of Technology)**

##### **Online/Internet Services** (continued)

**Note:** 20 USC 6777 and 47 USC 254 require districts receiving federal Title II technology funds or E-rate discounts to enforce the operation of technology protection measures. The legislation clarified that nothing in the Children's Internet Protection Act shall be construed to require the tracking of individual students' or adults' Internet use; thus, it appears to be left to the discretion of districts and schools as to whether they wish to track Internet use through personally identifiable web monitoring software or other means. The following optional paragraph may be revised to reflect district practice.

To ensure proper use, the Superintendent or designee may monitor employee usage of technological resources, including the accessing of email and stored files. Monitoring may occur at any time without advance notice or consent. When passwords are used, they must be known to the Superintendent or designee so that he/she may have system access.

The Superintendent or designee shall establish administrative regulations and an Acceptable Use Agreement which outline employee obligations and responsibilities related to the use of District technology. He/she also may establish guidelines and limits on the use of technological resources. Inappropriate use may result in a cancellation of the employee's user privileges, disciplinary action, and/or legal action in accordance with law, Board policy, and administrative regulation.

The Superintendent or designee shall provide copies of related policies, regulations, and guidelines to all employees who use the District's technological resources. Employees shall be required to acknowledge in writing that they have read and understood the District's Acceptable Use Agreement.

##### **Online/Internet Services: User Obligations and Responsibilities**

Employees are authorized to use District equipment to access the Internet or other online services in accordance with Board policy, the District's Acceptable Use Agreement, and the user obligations and responsibilities specified below.

1. The employee in whose name an online services account is issued is responsible for its proper use at all times. Employees shall keep account information, home addresses, and telephone numbers private. They shall use the system only under the account number to which they have been assigned.
2. Employees shall use the system safely, responsibly, and primarily for work-related purposes.

## **Personnel - Certified-Non-Certified**

### **Rights, Responsibilities and Duties**

#### **Acceptable Computer Network Use (Employee Use of Technology)**

##### **Online/Internet Services: User Obligations and Responsibilities (continued)**

3. Employees shall not access, post, submit, publish, or display harmful or inappropriate matter that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or disparagement of others based on their race, ethnicity, national origin, sex, gender, sexual orientation, age, disability, religion, or political beliefs.
4. Employees shall not use the system to promote unethical practices or any activity prohibited by law, Board policy, or administrative regulations.
5. Employees shall not use the system to engage in commercial or other for-profit activities without permission of the Superintendent or designee.
6. Copyrighted material shall be posted online only in accordance with applicable copyright laws.
7. Employees shall not attempt to interfere with other users' ability to send or receive email, nor shall they attempt to read, delete, copy, modify, or forge other users' email.
8. Unless on the district's web site (intranet), employees shall not develop any classroom or work-related web sites, blogs, forums, or similar online communications representing the District or using District equipment or resources without permission of the Superintendent or designee. Such sites shall be subject to rules and guidelines established for District online publishing activities including, but not limited to, copyright laws, privacy rights, and prohibitions against obscene, libelous, and slanderous content. Because of the unfiltered nature of blogs not on the intranet, any such site shall include a disclaimer that the District is not responsible for the content of the messages. The District retains the right to delete material on any such online communications.
9. Users shall report any security problem or misuse of the services to the Building Principal who will notify the Superintendent if necessary in writing.

## **Personnel - Certified-Non-Certified**

### **Rights, Responsibilities and Duties**

#### **Acceptable Computer Network Use (Employee Use of Technology)**

- (cf. 1311.1 – Political Activities/Functions of School Employees)
- (cf. 4118.4/4218.4 – E-Mail (Electronic Monitoring (staff))
- (cf. 4131 – Staff Development)
- (cf. 5125 – Student Records)
- (cf. 6141 – Curriculum Design/Development/Revision)
- (cf. 6141.32 – Computer Literacy)
- (cf. 6141.321 – Student Acceptable Use of the Internet)
- (cf. 6141.322 – Websites/Pages)
- (cf. 6141.323 – Internet Safety Policy/Filtering)

Legal References: Connecticut General Statutes

The Freedom of Information Act

53A-182B Harassment in the first degree.

P.A. 98-142 An Act Requiring Notice to Employees of Electronic Monitoring by Employers.

United States Code, Title 20

675 1-6777 Enhancing Education Through Technology Act, Title II, Part D, especially: 6777 Internet safety

United States Code, Title 47

254 Universal service discounts (E-rate)

Code Of Federal Regulations, Title 47

54.520 Internet safety policy and technology protection measures, E-rate discounts

Policy adopted: June 1, 2006  
Policy revised: June 18, 2009

NEW FAIRFIELD PUBLIC SCHOOLS  
New Fairfield, Connecticut

## **Personnel – Certified/Non-Certified**

### **Rights, Responsibilities, and Duties**

#### **Acceptable Computer Network Use**

The intent of these administrative regulations rules is to provide employees with general requirements for utilizing the school unit’s computers, networks, and Internet services. The administrative regulations may be supplemented by more specific administrative procedures and rules governing day-to-day management and operation of the computer system.

These rules provide general guidelines and examples of prohibited uses for illustrative purposes but do not attempt to state all required or prohibited activities by users. Employees who have questions regarding whether a particular activity or use is acceptable should seek further guidance from the office of the Assistant Superintendent.

Failure to comply with Board policy 4118.5/4218.5, these regulations and/or other established procedures or rules governing computer use may result in disciplinary action, up to and including discharge. Illegal uses of the school unit’s computers will also result in referral to law enforcement authorities.

#### **A. Access to School Computers, Networks, and Internet Services**

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

#### **B. Acceptable Use**

Employee access to the school unit’s computers, networks, and Internet services is provided for administrative, educational, communication, and research purposes consistent with the school unit’s educational mission, curriculum, and instructional goals. General rules and expectations for professional behavior and communication apply to use of the school unit’s computers, networks, and Internet services.

Employees are to utilize the school unit’s computers, networks, and Internet services for school-related purposes and performance of job duties. Incidental personal use of school computers is permitted as long as such use does not interfere with the employee’s job duties and performance, with system operations, or other system users. “Incidental personal use” is defined as use by an individual employee for occasional personal business. Employees are reminded that such personal use must comply with this policy and all other applicable policies, procedures, and rules.

#### **C. Prohibited Use**

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

## **Personnel – Certified/Non-Certified**

### **Rights, Responsibilities, and Duties**

#### **Acceptable Computer Network Use (continued)**

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 or minors;
4. Any use for 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 for-profit or not-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 building principal or appropriate administrator.
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 without permission from the office of the Assistant Superintendent;
8. Opening or forwarding any E-mail attachments (executable files) from unknown sources and/or that may contain malicious codes;
9. Sending mass E-mails to school users or outside parties for school or non-school purposes without the permission of the Assistant Superintendent;
10. Any malicious use or disruption of the school unit's computers, networks, and Internet services 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;
15. Failing to report a known breach of computer security to the office of the Assistant superintendent;
16. Using school computers, networks, and Internet services after such access has been denied or revoked; and
17. Any attempt to delete, erase, or otherwise conceal any information stored on a school computer that violates these rules.

## **Personnel – Certified/Non-Certified**

### **Rights, Responsibilities, and Duties**

#### **Acceptable Computer Network Use (continued)**

##### **D. No Expectation of Privacy**

The school unit retains, control, custody, and supervision of all computers, networks, and Internet 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, employee volunteers become aware of student violations, they are expected to stop the activity and inform the building principal or his/her designee.

##### **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 policy 4118.5/4218.5 and/or these regulations.

##### **H. School Unit Assumes No Responsibility for Unauthorized Charges, Costs, 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 its computers such as copyright violations.

**Personnel – Certified/Non-Certified**

**Rights, Responsibilities, and Duties**

**Acceptable Computer Network Use (continued)**

**Employee Acknowledgment Required**

Each employee authorized to access the school unit's computers, networks, and Internet services is required to sign an acknowledgment form stating that they have read policy 4118.5/4218.5 and these regulations. The acknowledgment form will be retained in the employee's personnel file.

Regulation approved:  
Regulation revised:

June 1, 2006  
June 18, 2009

NEW FAIRFIELD PUBLIC SCHOOLS  
New Fairfield, Connecticut



**NEW FAIRFIELD PUBLIC SCHOOLS  
New Fairfield, Connecticut**

**EMPLOYEE COMPUTER AND INTERNET USE  
ACKNOWLEDGMENT FORM**

No employee shall be allowed to use school computers or the Internet until s/he has signed and returned this acknowledgment.

I have read policy 4118.5/4218.5 – Acceptable Computer Network Use and its Administrative Regulations –Acceptable Computer Network Use and understand their terms and conditions.

---

Signature

---

Date