

Policy Subcommittee Meeting

Wednesday, February 22, 2023 7:00 PM

BOE Central Office Conference Room, 3 Brush Hill Road, New Fairfield, CT
06812

I. CALL TO ORDER

II. APPROVAL OF MINUTES

II.A. December 14, 2022 - Regular

III. ACTION ITEMS

III.A. Policy 3517.1 – Identification Badges

III.B. Policy 4118.5 – Acceptable Computer Network
Use

III.C. Policy 5118.111 – Tuition for Students of Staff
Members

III.D. Policy 6141.321 – Computers: Acceptable Use
and Internet Safety Policy

IV. INFORMATION ITEMS

V. OTHER

VI. ADJOURNMENT

BOARD OF EDUCATION, NEW FAIRFIELD, CT
Policy Subcommittee Meeting

Name of Subcommittee: Policy Meeting type: Regular
Date of Meeting: 12/14/22 Place of Meeting: Zoom
Members present: Kathy Baker, Samantha Mannion, Amy Johnson, Stephanie Strazza
Members absent:
Other attendees: Ken Craw, James D'Amico, Karen Gruetzner, Tim Blair, Dom Cipollone, Ed Sbordone
Minutes submitted by: Kathy Baker
Meeting Access: Policy Subcommittee (12/14/22 at 6 p.m.) Web: <https://zoom.us/j/97644209101>
Dial In: (929) 205-6099 Meeting ID: 976 4420 9101

The meeting was called to order at 6 p.m.

II. APPROVAL OF MINUTES

A. November 16, 2022 - Regular

Motion: To approve the minutes of November 16, 2022, as presented

Made by: Kathy Baker

Seconded by: Stephanie Strazza

Recording of Vote: All in favor

III. ACTION ITEMS

A. Policy 5132 – Dress and Grooming – Revision - Change to *Principal or their designee* instead of Principal or Assistant Principal in paragraphs five and six. This policy applies to all school sponsored activities. Students who continue to violate this policy would be dealt with under the school code of conduct manual. No restrictions on freedom of dress, grooming and adornment.

Motion: To move Policy 5132 - Dressing and Grooming to the full Board for approval

Made by: Samantha Mannion

Seconded by: Kathy Baker

Recording of Vote: All in favor

IV. INFORMATION ITEMS

A. Policy 5118.111 – Tuition for Students of Staff Members – The committee discussed adding SROs to the policy.

Motion: To keep Policy 5118.111 on the agenda and bring to the full Board

Made by: Samantha Mannion

Seconded by: Kathy Baker

Recording of Vote: All in favor – Kathy Baker, Samantha Mannion and Stephanie Strazza
Opposed – Amy Johnson

B. Vaping Update - A multi-pronged approach was discussed. James D'Amico did a poll of the SWC schools on detectors. Two of ten schools use vape detectors, one in permanent way and one in a pilot. Both cases are in a silent manner. They get five to ten pings a day with the detectors. Depending on the technology, there is a question on reliability. Both schools have slightly different conduct codes than ours and address the addiction piece with requiring the student to meet with a health counselor and suspension. The subcommittee agreed to put this topic back on the agenda for the next meeting.

V. OTHER – The subcommittee members would like to revisit the lanyards and badges policy with the middle school.

VI. ADJOURNMENT

Motion to adjourn: Made by: Kathy Baker

Seconded by: Samantha Mannion

Recording of vote: All in favor

Meeting adjourned at: 7:03 p.m.

Business/Non-Instructional Operations

Security of Buildings and Grounds

Site and Building Access

Identification Badges

The Board of Education recognizes the importance of providing a safe environment for all District students and staff. To promote a safe environment, the District requires all employees, volunteers and visitors to wear, above the waist, a District issued, approved identification badge.

Required Identification: All employees, while carrying out regular employment duties, will display identification badges in plain view. Student ID badges and lanyards will be provided to all students at the middle school and high school, which authorizes students to be on campus and on school buses. Students are asked to display their ID badge in a prominent location and to retain their ID badge. These ID badges will help staff in identifying students. Students will be required to present their ID badge to enter the school building if they arrive after the start of the school day.

Issuing Identification Badges: Identification badges will be provided to all employees. The initial badge, clip or lanyard will be provided to all employees at no cost to the employee. ID badges will be replaced as necessary due to normal use, to make the photo current or for changes in employment status.

Visitors/Volunteers: All visitors/volunteers are required to check in to the main office or front desk to obtain a visitor's badge. Volunteer and visitor badges may be permanent and lent to the person or disposable. A log shall be maintained of all visitors/volunteers in the building. When visitors/volunteers leave the building, they must sign out.

All visitors shall display the visitor's badge while they are in the school building during the school day.

Visitors who do not comply with this policy shall be escorted from the property. Staff members who observe someone entering District facilities without proper identification are required to address the person or immediately report this circumstance to the administration main office or front desk.

Lost or Stolen Badges: The first time the identification badge is lost or stolen, the District will provide a replacement at no cost. Each additional identification badge requested will cost \$10.00 per badge. If a badge is lost or stolen, employees should contact Human Resources and students should contact the school main office immediately.

(cf. 1250 – Visits to the School)

(cf. 3516 – Safety)

Business/Non-Instructional Operations

Security of Buildings and Grounds

Site and Building Access

Identification Badges

Legal Reference: Connecticut General Statutes

10-221 Boards of education to prescribe rules, policies and procedures.

Policy adopted: December 19, 2013
Policy revised: April 3, 2014
Policy revised: June 4, 2015
Policy revised: March 3, 2022

NEW FAIRFIELD PUBLIC SCHOOLS
New Fairfield, Connecticut

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

Students

Non-Resident Students

Tuition for Students of Staff Members

Non-resident staff employed by the New Fairfield Public Schools shall be allowed to have their child(ren) attend the New Fairfield Public Schools on a space available basis, subject to the following stipulations:

- The non-resident staff will be permitted to enroll their child only during the time of employment in the New Fairfield Public Schools.
- Nonresident staff will pay tuition for their children's enrollment in New Fairfield Public Schools. The tuition will be 15%* of the annual Sherman tuition rate established by the New Fairfield Board of Education. Students attending New Fairfield High School will pay 20%* of the annual Sherman tuition rate due to the greater cost associated with educating students in the 9-12 grade range. Payment of the tuition shall be made upon admission prorated for the length of time remaining in the school year.
- Staff members hired before the 2021-22 school year are exempt from paying tuition for their children.
- The nonresident staff will pay, in entirety, any extra costs beyond the regular school program that are directly attributable to their children.
- The Board will not "exclude a qualified handicapped child if the child can be provided an appropriate education." Except in the cases of children with "504 Plans," the Board will charge the nonresident staff member for the provision of special education and/or related services if that education or those services exceed the school district's annual Sherman tuition rate. If the district is unable to implement the IEP or 504 as written, the student may not enroll.
- The non-resident staff will be responsible for the transportation of their children to and from school.
- Non-resident staff will not be allowed to enroll any child who is currently excluded by expulsion from another public or private school.
- The Superintendent of Schools, in conjunction with the Principal of the school at which the student attends, can, with a minimum of two weeks' notice, terminate the program with an individual student for just and appropriate causes as determined by the Superintendent.
- Request for participation in this program must be made annually by the teacher on behalf of their child and, therefore, would require the annual review and approval of the Superintendent prior to continuing the following year.
- Children of non-resident staff will not be counted in New Fairfield's enrollment numbers for budgetary purposes.
- Any student accepted into this program will be given all of the rights, privileges, responsibilities and requirements of any other student in the school district.
- High School student athletes must abide by CIAC transfer regulations.

(*Tuition rates - subject to change)

Students

Non-Resident Students

Tuition for Students of Staff Members

Legal References: Connecticut General Statutes

10-76d Duties and powers of boards of education to provide special education programs and services.

10-253 School privileges for children in certain placements, nonresident children and children in temporary shelters.

34 CFR 104.39

Policy adopted: March 3, 2011
Policy revised: June 3, 2021

NEW FAIRFIELD PUBLIC SCHOOLS
New Fairfield, Connecticut

Students

Non-Resident Students

Tuition for Students of Staff Members and School Resource Officers (SROs) Assigned to the School District

Non-resident staff employed by the New Fairfield Public Schools and SROs assigned to the District shall be allowed to have their child(ren) attend the New Fairfield Public Schools on a space available basis, subject to the following stipulations:

- The non-resident staff will be permitted to enroll their child only during the time of employment in the New Fairfield Public Schools. An SRO assigned to the District shall be permitted to enroll their child only during the period of their assignment to the New Fairfield Public Schools.
- Nonresident staff and SROs assigned to the District will pay tuition for their children's enrollment in New Fairfield Public Schools. The tuition will be 15%* of the annual Sherman tuition rate established by the New Fairfield Board of Education. Students attending New Fairfield High School will pay 20%* of the annual Sherman tuition rate due to the greater cost associated with educating students in the 9-12 grade range. Payment of the tuition shall be made upon admission prorated for the length of time remaining in the school year.
- Staff members hired before the 2021-22 school year are exempt from paying tuition for their children.
- The nonresident staff will pay, in entirety, any extra costs beyond the regular school program that are directly attributable to their children.
- The Board will not "exclude a qualified handicapped child if the child can be provided an appropriate education." Except in the cases of children with "504 Plans," the Board will charge the nonresident staff member for the provision of special education and/or related services if that education or those services exceed the school district's annual Sherman tuition rate. If the district is unable to implement the IEP or 504 as written, the student may not enroll.
- The non-resident staff will be responsible for the transportation of their children to and from school.
- Non-resident staff and SROs assigned to the District will not be allowed to enroll any child who is currently serving a period of expulsion from another public or private school.
- The Superintendent of Schools, in conjunction with the Principal of the school at which the student attends, can, with a minimum of two weeks' notice, terminate the program with an individual student for just and appropriate causes as determined by the Superintendent.
- Request for participation in this program must be made annually by the teacher on behalf of their child and, therefore, would require the annual review and approval of the Superintendent prior to continuing the following year.
- Children of non-resident staff will not be counted in New Fairfield's enrollment numbers for

budgetary purposes.

- Any student accepted into this program will be given all of the rights, privileges, responsibilities and requirements of any other student in the school district.
- High School student athletes must abide by CIAC transfer regulations.

(*Tuition rates - subject to change)

Legal References: Connecticut General Statutes

[10-76d](#) Duties and powers of boards of education to provide special education programs and services.

[10-253](#) School privileges for children in certain placements, nonresident children and children in temporary shelters.

34 CFR 104.39

Policy adopted: March 3, 2011

Policy revised: June 3, 2021

NEW FAIRFIELD PUBLIC SCHOOLS

New Fairfield, Connecticut

Instruction

Computers: Acceptable Use and Internet Safety Policy

The school district is pleased to make available to students access to interconnected computer systems within the district and to the Internet, the worldwide network that provides various means of accessing significant educational materials and opportunities.

The District recognizes its responsibility to educate students regarding appropriate behavior on social networking and chat room sites about cyberbullying. Therefore, students shall be provided instruction about online behavior, including interacting with other individuals on social networking sites and in chat rooms and cyberbullying awareness and response.

In order for the school district to be able to continue to make its computer network and Internet access available, all students must take responsibility for appropriate and lawful use of this access. Students must understand that one student's misuse of the network and Internet access may jeopardize the ability of all students to enjoy such access. While the school teachers and other staff will make reasonable efforts to supervise student use of network and Internet access, they must have student cooperation in exercising and promoting responsible use of this access.

Below is the Acceptable Use and Internet Safety Policy ("policy") of the school district. Upon reviewing, signing, and returning this policy as the students have been directed, each student will be given the opportunity to enjoy Internet access at school. If a student is under 18 years of age, s/he must have his or her parents or guardians read and sign the policy. The school district cannot provide access to any student who, if 18 or older, fails to sign and submit the policy to the school as directed or, if under 18, does not return the policy as directed with the signatures of the student and his/her parents or guardians.

Listed below are the provisions of your agreement regarding computer network and Internet use. If you have any questions about these provisions, you should contact the person that your school has designated as the one to whom you can direct your questions. If any user violates this policy, the student's access will be denied, if not already provided, or withdrawn and s/he may be subject to additional disciplinary action.

Personal Responsibility

By signing this policy, you are agreeing not only to follow the rules in this policy, but reaffirming your responsibility to report any misuse of the network to the person designated by the school for such reporting. Misuse means any violations of this policy or any other use that is not included in the policy, but has the effect of harming another or his or her property.

All users are hereby made aware that all information on the New Fairfield Board of Education's computers, computer systems, and networks are in the public domain, unless specifically protected by Connecticut Freedom of Information Act.

The New Fairfield Board of Education reserves the right to bypass any or all individual group passwords to determine the activity on any or all computers, computer systems, software, electronic access privileges, and networks.

Instruction

Computers: Acceptable Use and Internet Safety Policy (continued)

Term of the Permitted Use

A student who submits to the school, as directed, a properly signed policy and follows the policy to which s/he has agreed will have computer network and Internet access during the course of the school year only. Parents/students must sign a responsible use agreement for electronic information resources upon entering Consolidated School, Meeting House Hill School, New Fairfield Middle School and New Fairfield High School before students are given an access account.

Acceptable Uses

1. **Educational Purposes Only.** The school district is providing access to its computer networks and the Internet for only educational purposes. If you have any doubt about whether a contemplated activity is educational, you may consult with the person(s) designated by the school to help you decide if a use is appropriate.
2. **Unacceptable Uses of Network.** Among the uses that are considered unacceptable and that constitute a violation of this policy are the following:
 - A. Uses that violate the law or encourage others to violate the law. Don't transmit offensive or harassing messages; offer for sale or use any substance the possession or use of which is prohibited by the school district's student discipline policy; view, transmit, or download pornographic materials or materials that encourage others to violate the law; intrude into the networks or computers of others; and download or transmit confidential, trade secret information, or copyrighted materials. Even if materials on the networks are not marked with the copyright symbol, you should assume that all materials are protected unless there is explicit permission on the materials to use them.
 - B. Uses that cause harm to others or damage to their property. For example, don't engage in defamation (harming another's reputation by lies); employ another's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating or otherwise using his/her access to the network or the Internet; upload a worm, virus, "Trojan horse," "time bomb," or other harmful form of programming or vandalism; participate in "hacking" activities or any form of unauthorized access to other computers, networks, or information systems.
 - C. Uses that jeopardize the security of student access and of the computer network or other networks on the Internet. For example, don't disclose or share your password with others; don't impersonate another user.
 - D. Uses that are commercial transactions. Students may not sell or buy anything over the Internet. Students may not give others private information about themselves, including credit card numbers and social security numbers. Staff may make commercial transactions for educational or for research purposes as long as the transaction does not interfere with the employee's job duties and performance.

Instruction

Computers: Acceptable Use and Internet Safety Policy (continued)

3. **Computing Etiquette** All users must abide by rules of computing etiquette, which include the following:

- A. Be polite. Messages should not be abusive to others.
- B. Take pride in communications. Check spelling and grammar.
- C. Use appropriate language. Do not swear or use vulgarities or any other inappropriate language, symbols, or pictures.
- D. Protect password confidentiality. Passwords are not to be shared with others. Using another user's account or password or allowing such access by another may be permitted only with the approval of the supervising teacher or technology coordinator.
- E. Staff and students in grades 6-12 will be required to change their passwords every six months. This password change will be enforced by the system. Reminders will be sent out via email starting 30 days prior to expiration.

Passwords must meet the following complexity requirements: they must be at least 8 characters and contain at least one uppercase letter, one lowercase letter, one special character, and one numeral. Previously used passwords must not be used.

- F. Do not reveal your personal address, telephone number or e-mail address or those of other persons. No student information protected by FERPA should be electronically transmitted or otherwise disseminated through the network.
- G. Do not disguise the point of origin or transmission of electronic mail.
- H. Do not send messages that contain false, malicious, or misleading information that may be injurious to a person or a person's property.
- I. Illegal activities are strictly prohibited.
- J. The district technology is not to be used for playing multi-user or other network intensive games, commercial ventures, Internet relay chat lines, or downloading excessively large files.
- K. No charges for services, products, or information are to be incurred without permission of the supervising teacher or technology coordinator.
- L. Do not use the network in such a way that you would disrupt the use of the network by other users.
- M. Users shall respect the privacy of others and not read the mail or files of others without their permission. Copyright and licensing laws will not be intentionally violated.
- N. Vandalism will result in cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy hardware, data of another user, Internet, or any other agencies or other networks which may be accessed. This includes, but is not limited to, the uploading or creation of computer viruses.

Instruction

Computers: Acceptable Use and Internet Safety Policy (continued)

- O. Report security problems to the supervising teacher or technology coordinator.
- P. Violators of this policy shall hold the district, including its employees and agents, harmless against any and all causes of action, damages, or other liability resulting from the willful or negligent violation of this policy.

Internet Safety

1. **General Warning; Individual Responsibility of Parents and Users.** All users and their parents/guardians are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged students. Every user must take responsibility for his or her use of the computer network and Internet and stay away from these sites. Parents of minors are the best guides of materials to shun. If a student finds that other users are visiting offensive or harmful sites, s/he should report such use to a teacher or administrator.
2. **Personal Safety.** Be safe. In using the computer network and Internet, do not reveal personal information such as your home address, telephone number or e-mail address. Do not use your real last name or any other information which might allow a person to locate you without first obtaining the permission of a supervising teacher. Do not arrange a face-to-face meeting with someone you “meet” on the computer network or Internet without your parent’s permission (if you are under 18). Regardless of your age, you should never agree to meet a person you have only communicated with on the Internet in a secluded place or in a private setting.

“Hacking” and Other Illegal Activities. It is a violation of this policy to use the school’s computer network or the Internet to gain unauthorized access to other computers or computer systems, or to attempt to gain such unauthorized access. Any use which violates state or federal law relating to copyright, trade secrets, the distribution of or pornographic materials, or which violates any other applicable law or municipal ordinance, is strictly prohibited.
3. **Confidentiality of Student Information.** Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian, or if the student is 18 or over, the permission of the student himself/herself. Users should never give out private or confidential information about themselves or others on the Internet, particularly credit card numbers and social security numbers. A supervising teacher or administrator may authorize the release of directory information, as defined by law, for internal administrative purposes or approved educational projects and activities.

Instruction

Computers: Acceptable Use and Internet Safety Policy

Internet Safety (continued)

4. **Active Restriction Measures.** The school, either by itself or in combination with the Data Acquisition Site providing Internet access, will utilize filtering software or other technologies to prevent students from accessing visual depictions that are (1) obscene, (2) child pornography, or (3) harmful to minors. The school will also monitor the online activities of students, through direct observation and/or technological means, to ensure that students are not accessing such depictions or any other material which is inappropriate for minors.

Internet filtering software or other technology-based protection systems may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by students age 18 and older.

The term “harmful to minors” is defined by the Communications Act of 1934 (47 USC Section 254 [h][7]), as meaning any picture, image, graphic image file, or other visual depiction that:

- Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
- 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;
- Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

Privacy

Network and Internet access are provided as a tool for your education. The school district reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the school district and no user shall have any expectation of privacy regarding such materials.

Failure to Follow Policy

The user’s use of the computer network and Internet is a privilege, not a right. A user who violates this policy, shall at a minimum, have his or her access to the computer network and Internet terminated, which the school district may refuse to reinstate for the remainder of the student’s enrollment in the school district. A user violates this policy by his or her own action or by failing to report any violations by other users that come to the attention of the user. Further, a user violates this policy if s/he permits another to use his or her account or password to access the computer network and Internet, including any user whose access has been denied or terminated. The school district may also take other disciplinary action in such circumstances.

Instruction

Computers: Acceptable Use and Internet Safety Policy (continued)

Warranties/Indemnification

The school district makes no warranties of any kind, either express or implied, in connection with its provision of access to and use of its computer networks and the Internet provided under this policy. It shall not be responsible for any claims, losses, damages, or costs (including attorney's fees) of any kind suffered, directly or indirectly, by any user or his or her parent(s) or guardian(s) arising out of the user's use of its computer networks or the Internet under this policy. By signing this policy, users are taking full responsibility for his or her use, and the user who is 18 or older, or in the case of a user under 18, the parent(s) or guardian(s) are agreeing to indemnify and hold the school, the school district, the Data Acquisition Site that provides the computer and Internet access opportunity to the school district and all of their administrators, teachers, and staff harmless from any and all loss, costs, claims, or damages resulting from the user's access to its computer network and the Internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user. The user, or if the user is a minor, the user's parent(s) or guardian(s) agree to cooperate with the school in the event of the school's initiating an investigation of a user's use of his or her access to its computer network and the Internet, whether that use is on a school computer or on another computer outside the school district's network.

Updates

Users, and if appropriate, the user's parent(s)/guardian(s), may be asked from time to time to provide new or additional registration and account information or to sign a new policy, for example, to reflect developments in the law or technology. Such information must be provided by the user (or his/her parent(s) or guardian(s)) or such new policy must be signed if the user wishes to continue to receive service. If after you have provided your account information, some or all of the information changes, you must notify the person designated by the school to receive such information.

(cf. 4118.5/4218.2 Acceptable Computer Network Use)

Legal Reference: Connecticut General Statutes
1-19(b)(11) Access to public records. Exempt records.
10-15b Access of parent or guardian to student's records.
10-209 Records not to be public.
11-8a Retention, destruction and transfer of documents.
11-8b Transfer or disposal of public records. State Library Board to adopt regulations.

Instruction

Computers: Acceptable Use and Internet Safety Policy

Legal References: Connecticut General Statutes (continued)
46b-56(e) Access to Records of Minors
Connecticut Public Records Administration Schedule V-Disposition of Education Records (Revised 1983).
Federal Family Educational Rights and Privacy Act of 1974 (section 438 of the General Education Provisions Act, as amended, added by section 513 of PL 93-568, codified at 20 U.S.C. 1232g.)
Dept. of Education 34 CFR. Part 99 (May 9, 1980 45 FR 30802) regs. Implementing FERPA enacted as part of 438 of General Education Provisions Act (20 U.S.C. 1232g)-parent and student privacy and other rights with respect to educational records, as amended 11/21/96.
Children’s Internet Protection Act of 2000 (HR 4577, P.L. 106-554)
Communications Act of 1934, as amended (47 U.S.C. 254[h].[I])
Elementary and Secondary Education Act of 1965, as amended (20 U.S.C. 6801 et seq., Part F)
Public Law 94-553, The Copyright Act of 1976, 17 U.S.C. 101 et. Seq.
Reno v ACLU, 521 U.S.844(1997)
Ginsberg v. New York, 390 U.S. 629, at 642, n.10 (1968)
Board of Education v. Pico, 457 U.S. 868 (1988)
Hazelwood School District v. Kuhlmeier, 484 U. 620, 267 (1988)
Public Law 110-385 Broadband Data Improvement Act/Protecting Children in the 21st Century Act

Policy adopted: January 4, 2007
Policy revised: January 15, 2009
Policy revised: November 17, 2011
Policy revised: August 2, 2012
Policy revised: June 5, 2014
Policy revised: November 2, 2016
Policy revised: June 21, 2018

NEW FAIRFIELD PUBLIC SCHOOLS
New Fairfield, Connecticut

Instruction

Computers: Acceptable Use and Internet Safety

Acceptable Electronic Resources Use

1. Privilege

The use of the New Fairfield Public School electronic resources is a privilege. Inappropriate use, depending upon the severity, can result in temporary suspension or cancellation of this privilege and/or disciplinary/legal action ranging from detention to possible suspension and/or expulsion of a student and disciplinary action, including discharge of an employee.

2. Personal Responsibility

Individuals will accept personal responsibility for reporting any misuse or vandalism of electronic resources. Student(s) faculty/staff member(s) and network guest(s) will not assist another in violating any of these responsibilities:

- Misuse of the electronic resources shall occur when messages or materials are sent and/or requested within/from outside the network that attack ethnic, religious or racial groups or indicate pornography, unethical or illegal activities, sexism, harassment or inappropriate language.
- Vandalism or any malicious attempt to harm or destroy any school equipment, service or data of another user or any other networks that are connected to the system. This includes, but is not limited to, tampering with computer hardware and software, uploading or creating computer viruses, vandalizing/modifying data without permission or attempting to gain access to restricted or unauthorized networks or network services.

3. Acceptable Use

The use of electronic resources must be in support of education and research in accordance with the educational goals and objectives of New Fairfield Public Schools. All users are personally responsible for:

- a. complying with the rules appropriate to each school's network system.
- b. refraining from transmitting, receiving or duplicating any material in violation of any United States or state laws (this includes, but is not limited to copyrighted material; threatening, harassing or obscene material or material protected by trade secret).
- c. refraining from illegally using copyrighted materials. This includes, but is not limited to, improper use of license user requirements or using personal/borrowed software on the network.

Instruction

Computers: Acceptable Use and Internet Safety

Acceptable Electronic Resources Use

3. Acceptable Use (continued)

- d. refraining from soliciting others for commercial, religious or political causes, outside organizations or personal matters.

4. Network Etiquette and Privacy

Network behavior and language should be consistent with school/classroom standards. These rules include, but are not limited to, the following:

- a. **Be Polite** - Never send, or encourage others to send abusive, harassing or inappropriate messages and/or materials.
- b. **Use Appropriate Language** - Never swear, use vulgarities or any other inappropriate language.
- c. **Privacy** - Do not reveal any personal, confidential or sensitive information (i.e. addresses or phone numbers of yourself or others). Published student work will be identified by first name (last name initial, if necessary) and grade level, photos will consist only of groups and will be blurred for web pages. If student photos, audio or video will be used in a media/electronic based presentation or major school event, a media/electronic release form will be sent home prior to the presentation or event to obtain permission.
- d. **Login ID/Password** - Do not share personal login ID/passwords with anyone. If someone has learned a personal login ID/password, please alert the network administrator.

Staff and students in grades 6-12 will be required to change their passwords every six months. This password change will be enforced by the system. Reminders will be sent out via email starting 30 days prior to expiration.

Passwords must meet the following complexity requirements: they must be at least 8 characters and contain at least one uppercase letter, one lowercase letter, one special character, and one numeral. Previously used passwords must not be used.

- e. **Electronic Mail** - Do not send personal messages, of any kind, at any time. Messages relating to or in support of illegal activities must be reported to the authorities.
- f. **Disruptions** - Do not use the network in any way that would disrupt use of the network by others.
- g. **Published Resources** - Only copy published resources for the purpose of private study, scholarship or research. Material copied under these guidelines must include an appropriate citation of its source.

Instruction

Computers: Acceptable Use and Internet Safety

Acceptable Electronic Resources Use (continued)

5. Security

Due to the large amount of users, security is a high priority for those using the network system.

- a. Use only personal login ID/password.
- b. Do not enter any other account, whether it is assigned to another faculty/staff member, student, the school or the district without permission.
- c. If a security problem arises, notify the network administrator immediately, and do not demonstrate the problem to other users.

6. Ownership and Access

The New Fairfield Public School's network and computer facilities, associated hardware, software and peripherals, and all user files, electronic messages, data and programs stored, created or generated are the sole and exclusive property of the New Fairfield Public Schools ("Computer Facilities"). Any files, data or other information which is created, communicated or stored by any student or faculty/staff member of the New Fairfield Public Schools using Computer Facilities may be monitored to ensure that only appropriate business and education related tasks and messages are being performed and transmitted. Moreover, the student or faculty/staff member may not copy, reproduce or remove any files, data or equipment for any purpose without the prior approval of the New Fairfield Public School Technology Committee.

7. Services

New Fairfield Public Schools makes no warranties of any kind, whether expressed or implied, for the network service it is providing.

- a. New Fairfield Public Schools will not be responsible for any damages suffered while on this system. These damages may include but not limited to loss of data as a result of delays, non-deliveries, misdeliveries or service interruptions caused by the system or personal errors or omissions.
- b. Use of any information obtained via the network and other electronic resources is at one's own risk. Although precautions will be taken to attempt to ensure that the Internet is a safe learning environment, New Fairfield Public Schools specifically denies any responsibility for the accuracy, quality or content of information obtained through its Internet services.

Instruction

Computers: Acceptable Use and Internet Safety

Acceptable Electronic Resources Use

7. Services (continued)

All users agree to hold the New Fairfield School District, its faculty/staff, administrators and Board of Education harmless from any loss or damage that may occur as a result of the use of the school’s electronic resources.

Internet Use Permission - To ensure that only authorized students who understand the bounds of permitted use will have access to the Internet, New Fairfield Public Schools must obtain the written permission of a student’s parent or legal guardian before the student may access the Internet.

Review/Revision of Disciplinary Actions - Disciplinary actions related to technology will be periodically reviewed and revised by the District Technology Committee.

Regulation approved: October 18, 1998
Regulation reviewed: January 15, 2009
Regulation reviewed: November 17, 2011
Regulation reviewed: June 5, 2014
Regulation reviewed: November 2, 2016
Regulation revised: June 21, 2018

NEW FAIRFIELD PUBLIC SCHOOLS
New Fairfield, Connecticut

New Fairfield School District
Consolidated School

Responsible Use Agreement for Electronic Information Resources

Grades K-2

(Student's Name), _____, as a user of the New Fairfield School District's electronic information resources and computer networks, accept and agree to abide by the Acceptable Use and Internet Safety Policy of the New Fairfield Board of Education and with the following preconditions of my use:

1. I will use computers for educational purposes and always under the supervision of a staff member;
2. I will be polite and use only appropriate language;
3. I will not knowingly destroy computer programs or equipment belonging to the school;
4. I will not give out personal information about myself or to others when using the computer and Internet;
5. I will follow these rules. If I do not, I will not be permitted to use the computers and Internet at Consolidated School;
6. I will report all problems to my teacher or the school staff supervising my use of the computer;
7. I have read these rules and have discussed them with my child. We agree on the importance and necessity of this agreement in the new Information Age.

Student's Signature: _____ Date: _____

Parent's/Guardian's Signature: _____ Date: _____

New Fairfield School District
Meeting House Hill School

Responsible Use Agreement for Electronic Information Resources

Access to and use of the Internet is a privilege that students must earn by using it in an appropriate manner. All Meeting House Hill students must read and agree to follow the rules listed below, as well as follow the school rules in the Student Handbook. As a user of the New Fairfield school district's electronic information resources and computer networks, I accept and agree to abide by the Acceptable Use and Internet Safety Policy of the New Fairfield Board of Education and with the following preconditions of my use:

1. I will use electronic information resources only with the permission of a teacher.
2. I will use the Internet only for school educational and research purposes.
3. I will not make any changes to the computer software system set-up or data or open any software files without permission. I understand that any vandalism will result in disciplinary consequences.
4. I will not subscribe to any group on the Internet without a teacher's permission.
5. I will get permission from a teacher before printing.
6. If any site I visit contains inappropriate* words or pictures I will inform a teacher and immediately "back out" of the site.

**Inappropriate refers to obscene and/or offensive language, graphic sexual materials or illegal materials.*

7. I will not give out personal information about myself or others when using the Internet.

Student's Signature: _____ Date: _____

Parent's/Guardian's Signature: _____ Date: _____

Responsible Use Agreement for Electronic Information Resources

New Fairfield School District
New Fairfield High School and New Fairfield Middle School

Responsible Use Agreement for Electronic Information Resources

The school's information technology resources, including email and internet access, are provided for educational purposes. Adherence to the following policy is necessary for continued access to technology resources.

Students must respect and protect the privacy of others. During instructional time, devices are to be used for instructional purposes connected to the approved curriculum, not to cheat on assignments or tests, not to make personal phone calls, not to send text messages, and not to post information, photos, or videos not authorized by the teacher. Private identifying information about yourself or others must not ever be shared.

Students must respect and protect the integrity, availability, and security of all electronic resources. Information should be shared as required through the curriculum. Any security risks or violations must be reported to a teacher immediately.

Students must respect and protect the intellectual property of others. Copyright laws are to be understood and followed. Unauthorized copying of the intellectual property of others is a violation of this policy.

Students must respect and practice the principles of community. Communication in ways that are kind and respectful is expected. Threatening, discomfoting, and illegal materials that violate the school's code of conduct (such as obscenities; pornography; and threatening, rude, discriminatory, or harassing information) are unacceptable. Spam, chain letters, and any mass mailings are prohibited. Buying, selling, advertising, or otherwise conducting business is not allowed, unless approved as a part of the curriculum.

As a user of the New Fairfield school district's electronic information resources and computer networks, which includes student email access, I accept and agree to abide by the Acceptable Use and Internet Safety Policy of the New Fairfield Board of Education and with the following preconditions of my use:

1. I will use electronic information resources only for educational, research, and communication purposes and only as those purposes are consistent with the educational objectives of the New Fairfield Board of Education.
2. I will use electronic information resources in a responsible, ethical, and legal manner at all times.
3. I will use polite and appropriate language at all times while accessing and using these resources.

4. I will not give out any personal information about myself or anyone else while using these resources other than my first name and school e-mail address.
5. I will not knowingly degrade or disrupt electronic information resources, services or equipment, and I understand that such activity may be considered to be a crime and includes, for example, tampering with computer hardware and software, vandalizing or modifying data without permission, invoking computer viruses, attempting to gain access to restricted or unauthorized networks or network services and installing unauthorized software on the district's computers.
6. I will not cause harm to others or damage to their property (e.g., engage in defamation, gain or use passwords belonging to others, participate in "hacking" activities).
7. I will not jeopardize the security of student access and the computer network(s).
8. I will not violate any copyright laws. Even if the material on the networks is not marked with the copyright symbol. I will assume that all materials are protected unless there is explicit permission on the materials to use them. Plagiarism will not be tolerated.
9. I will not transmit, receive, or publish any threatening or obscene material.
10. I will not play unauthorized games or participate in unauthorized chat rooms.
11. I will not download any files to the hard drive without the permission of a staff member.
12. I will not subscribe to list serves or news groups.
13. I will not use the resources for commercial purposes, product advertising, or political lobbying and/or campaigning. Students may not sell or buy anything over the Internet.
14. If I do not follow these rules, I know that I may lose my privilege to use the computers at school, that I may be disciplined for not following the rules, and that I may have to pay for any damage I cause by my misuse of these resources.
15. I am aware that the inappropriate use of these resources can be a violation of local, state, and federal laws and that I may be prosecuted for violating those laws.
16. I will immediately report any problems or breaches of these responsibilities or any inappropriate messages received to my teacher or to the school personnel who is supervising my use of these resources.
17. I will act responsibly at all times and will avoid all other activities that are considered to be inappropriate in the non-electronic school environment.
18. If I violate this policy, I am subject to having my access to the computer network and Internet terminated, which the school district may refuse to reinstate for the remainder of my enrollment in the school district.

Parents, please discuss these rules with your student to ensure that s/he understands them. These rules also provide a good framework for your student's use of computers at home. For more information, see <http://www.justice.gov/criminal/cybercrime/cyberethics.htm>

**New Fairfield School District
New Fairfield High School and New Fairfield Middle School**

Every high school and middle school student, regardless of age, must read this page. If a student wants to use the school's network resources outside of network opportunities provided during teacher directed classroom instruction, then this form must be signed below.

I have read, understand, and agree to abide by the terms of the foregoing Acceptable Use and Internet Safety Policy. Should I commit any violation or in any way misuse my access to the school district's computer network and the Internet, I understand and agree that my access privilege may be revoked and school disciplinary action may be taken against me.

User's name (print clearly) _____ Home phone _____

User's signature _____ Date _____

Address _____

Status: Student Staff Patron

Parent or Guardian: As the parent or legal guardian of the above student, I have read, understand, and agree that my child or ward shall comply with the terms of the school district's Acceptable Use and Internet Safety Policy for the student's access to the school district's computer network and the internet. I understand that access is being provided to the students for educational purposes only. However, I also understand that it is impossible for the school to restrict access to all offensive and controversial materials and understand my child's or ward's responsibility for abiding by the policy. I am, therefore, signing this policy and agree to indemnify and hold harmless the school, the district, and the Data Acquisition Site that provides the opportunity to the school district for computer network and Internet access against all claims, damages, loses, and costs, or whatever kind that may result from my child's or ward's use of his or her access to such networks or his or her violation of the foregoing policy. Further, I accept full responsibility for supervision of my child's or ward's use of his or her access account if and when such access is not in the school setting. I hereby give permission for my child or ward to use the building-approved account to access the school district's computer network and the Internet.

Parent's/Guardian's name (please print): _____ Phone: _____

Parent's/Guardian's signature: _____ Date: _____

Address: _____