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

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)

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. 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, 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 Superintendent or designee.

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: August 21, 2023

THOMASTON PUBLIC SCHOOLS
Thomaston, CT

Personnel - Certified-Non-Certified

Rights, Responsibilities and Duties

Acceptable Computer Network Use

The Board of Education provides computers, networks and Internet access to support the educational mission of the schools and to enhance the curriculum and learning opportunities for students and school staff.

Employees are to utilize the district's computers, networks, email system and Internet services for school-related purposes and performance of job duties. Limited incidental personal use of district computers, networks, email systems and Internet services 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. "Limited incidental personal use" is defined as use by an individual employee for an appropriate, lawful, brief and occasional personal purposes. Employees are reminded that such personal use must comply with this policy and all other applicable policies, procedures and rules.

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. The systems' security aspects, message delete function and personal passwords can be bypassed for monitoring purposes. Therefore, employees must be aware that they should not have any expectation of personal privacy in the use of these computer systems. This provision applies to any and all uses of the district's computer systems, including any incidental personal use permitted in accordance with this policy and applicable regulations.

Online/Internet Services

The Board will educate minor students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber-bullying awareness and response. Additionally, the Board will implement a technology protection measure to block or filter Internet access to visual depictions that are obscene material, contain child pornography, or are harmful to minors and ensure that such filtering technology is operative during computer use by minor students.

Personnel - Certified-Non-Certified

Rights, Responsibilities and Duties

Acceptable Computer Network Use (continued)

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

All District computers remain under the control, custody and supervision of the school district. The school unit reserves the right to monitor all computer and Internet activity by employees. Employees have no expectation of privacy in their use of school computers.

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

The Superintendent or his/her designee 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/regulations. The Superintendent or his/her designee may develop additional administrative procedures/rules governing the day-to-day management and operations of the school district's computer system as long as they are consistent with the Board's policy/rules. The Superintendent may delegate specific responsibilities to building principals and others as he/she deems appropriate.

(cf. 6141.321 - Student Use of the Internet)
(cf. 6141.322 - Web Sites/Pages)

Legal References: Connecticut General Statutes
The Freedom of Information Act
31-48d Employers engaged in electronic monitoring required to give prior notice to employees. Exceptions. Civil penalty.
53a-182 Disorderly conduct; Class C misdemeanor
53a-182b Harassment in the first degree.
53a-183 Harassment in the second degree
53a-250 Computer-related Offenses: Definitions
Electronics Communication Privacy Act, 28 U.S.C. §2510 through 2520

Policy adopted: August 21, 2023

THOMASTON PUBLIC SCHOOLS
Thomaston, CT