Personnel - Certified-Non-Certified

Rights, Responsibilities and Duties

Acceptable Technology Use

Overview

The Stonington Board of Education (Board) provides its students and staff access to a multitude of technology resources. Access to information and communication technologies is considered a privilege and not a right. Technology resources consist of any technology and/or devices that access or convey information, software applications, Internet resources and Internet environments.

These resources provide opportunities to enhance learning and improve communication within our community and with the global community beyond the local campus. The advantages of having access to these resources are viewed by the Board as far greater than any potential downside. However, with the privilege of access is the responsibility of students, teachers, staff and the public to exercise appropriate personal responsibility in their use of these resources. The policies of the Board are intended to promote the most effective, safe, productive, and instructionally sound uses of networked information and communication tools.

Employees, contractors and guests ("Users") of Stonington Public Schools, are to utilize the district's computers, networks, email system and Internet services for school-related purposes and performance of job duties. Limited personal use of district computers, networks, email systems and Internet services is permitted as long as such use does not interfere with the 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. Users are reminded that such personal use must comply with this policy and all other applicable policies, procedures and rules.

Users shall be notified that computer files and electronic communications, including email and voicemail, 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 cyberbullying 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 students.

Any user 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 District reserves the right to monitor all computer and Internet activity by employees. Users have no expectation of privacy in their use of district technology resources.

Each employee authorized to access the school district's computers, networks and Internet services as required by their job will 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.

Expectations

Responsible use of the technology resources provided by the Board is expected to be ethical, respectful, academically honest, and supportive of the school's mission. Each computer user has the responsibility to respect every other person in our community and on the Internet. Digital storage and electronic devices used for school purposes will be treated as extensions of the physical school space. Administrators, or their designees, may review files and communications (including electronic mail) to insure that users are using the system in accordance with Board policy. Users should not expect that files stored on servers or disks will be private.

Some activities are expressly prohibited by law. Users are expected to abide by the generally accepted rules of network etiquette. The following guidelines are intended to clarify expectations for conduct, but they should not be construed as all-inclusive. Given the nature of emerging technologies, it is impossible to anticipate or prevent all problems that may occur.

- Use of electronic devices should be consistent with the Board's educational objectives, mission and curriculum.
- Transmission of any material in violation of any local, federal and state laws is prohibited. This includes, but is not limited to copyrighted material, licensed material and threatening or obscene material.
- Intentional or unintentional use of computing resources to access or process, proxy sites, pornographic material, explicit text or files, or files dangerous to the integrity of the network is strictly prohibited.
- Software and/or services may not be installed or downloaded on school devices without prior approval of the Superintendent or designee.
- Use of computing resources for commercial activities, product advertisement or religious or political lobbying is prohibited.
- Users may be held personally and financially responsible for malicious or intentional damage done to network software, data, user accounts, hardware and/or unauthorized costs incurred.
- Users may be held personally and financially responsible for damage to equipment outside of normal wear and tear.
- Files stored on district-managed networks are the property of the school district and, as such, may be inspected at any time and should not be considered private.

(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: October 12, 2017

STONINGTON PUBLIC SCHOOLS
Stonington, Connecticut