

Instruction**Instructional Resources****STUDENT INTERNET USE****6417**

~~Uses of electronic communication systems allow unprecedented opportunities for students to communicate, learn, access, and publish information. The district believes that the resources available through this network and the skills that students will develop in using it are of significant value in the learning process and student success in the future. These new opportunities also pose new challenges including, but not limited to, ready access for all students, age-level appropriateness of some material available through networks, security of the electronic communications system, and cost of maintaining increasingly complex networks. The district will endeavor to ensure that these concerns are appropriately addressed.~~

~~The district grants access to the network and the Internet by users only for the educational activities authorized under the administrative regulations including guidelines, procedures, and the specific limitations contained in this document.~~

~~The Fairfield Public Schools provide a variety of resources [District Technology Resources](#) in support of our instructional and administrative programs to ensure that our students become digital citizens proficient in [Information Technology Competencies](#) essential for success in the 21st century. These resources [District Technology Resources](#) enhance learning and improve communication within our local and global communities. The advantages of having access to these resources [District Technology Resources](#) exceed a potential disadvantage. However, access to them is a privilege and not a right. Therefore, it is incumbent upon all members of the school community to use [Technology District Technology Resources](#) responsibly, ethically and with respect for the work of others.~~

~~The District policies are intended to promote the most effective, safe, productive, and instructionally sound uses of technology resources [District Technology Resources](#), information and communication tools. The District also makes a good faith effort to protect its students from exposure to Internet materials that are harmful, inappropriate, or explicit. The District employs a system of Internet content filtering controls that meet federal standards established by the Children's Internet Protection Act (CIPA). Ultimately, parents and/or guardians of minors are responsible for setting and conveying the standard that their children should follow when using electronic media information resources [District Technology Resources](#).~~

~~To the extent that it is practical and prudent, ~~the~~ District will provide training and procedures that encourage the widest possible access to electronic information systems and networks [District Technology Resources](#) by students, staff, and patrons while establishing reasonable controls for the lawful, efficient, and appropriate use and management of the system.~~

Instruction

Instructional Resources

STUDENT INTERNET USE (continued)

6417

Use of the District's Technology Resources, and/or a student's personal electronic devices on school property or during a school sponsored or related activity, are expected to be lawful, ethical, respectful, academically honest, and supportive of the school's mission. Each student user of the District's Technology Resources, and/or of the student's personal electronic devices on school property or during school sponsored or related activity, has the responsibility to respect every other person in our community and on the Internet. All students are expected to follow the guidelines, procedures, and specific limitations outlined in the Acceptable Use Guidelines and Agreement (6417AR). Digital storage and electronic devices that are owned by the School District are District Technology Resources and are subject to search at any time.

Students are prohibited from using on school property or during a school sponsored or related activity, and/or connecting to a District network, District Technology Resources or any personal electronic devices for a use that is prohibited by this policy, other District or administrative policies, rules and regulations and/or state and federal law.

Personal electronic devices include, but are not limited to: cell phones, smart phones, tablets (Kindles, Nooks, iPads etc.), personal laptop computers, memory sticks, or any device or item that can or may be capable of receiving, transmitting and/or storing digital information or digital media.

If a student brings a personal electronic device onto school property or to a school sponsored or related activity and/or connects a personal electronic device to a District network, they are District Technology Resources, the student is subject to the rules and regulations regarding acceptable use that are contained in this policy, related District or policies and rules, administrative policies, regulations and rules, and/or state and federal law. Any use that is inconsistent in violation with of District policies the foregoing may result in loss of computer and internet privileges and/or other discipline commensurate with the offense.

By bringing a personal electronic device onto school property or to a school sponsored or related activity and/or connecting a personal electronic device to a District network District Technology Resources, the student consents that faculty may confiscate said device if the faculty has there is a reasonable suspicion that a student is using a personal electronic device in a manner that is inconsistent with this policy or with other District rules or administrative regulations, rules, or policies, and/or state and federal law. Depending on the situation, The school may search the electronic device in a manner and to an extent that is consistent with, and limited to the basis for the reasonable suspicion and

determining whether a violation of District policy and/or state and federal law has occurred.

Password systems implemented by the District are designed solely to provide system security from unauthorized users, not to provide privacy to the individual student.

- Use of District Technology Resources and personal ~~E~~electronic devices may only be used in a manner that is ~~should be~~ consistent with the District's educational objectives, mission and curriculum.
- Receipt, ~~T~~transmission and/or storage of any material in violation of District or administrative regulations, rules or policies, and/or any local, federal and or state law is prohibited. This includes, but is not limited to: copyrighted material, licensed material and threatening, harassing, or obscene material.
- Intentional or unintentional use of ~~computing resources~~ District Technology Resources to access or process proxy sites, pornographic or other inappropriate material, explicit text or files, or files dangerous to the integrity of the network and/or instructional resources is ~~strictly~~ prohibited.
- Use of ~~computing resources~~ District Technology Resources for commercial activities, or for solicitation not approved by the District, ~~product advertisement or religious or political lobbying~~ is prohibited.
- Students will utilize appropriate online behavior, including interactions with others in social media sites or chat rooms, and refrain from cyber-bullying behavior.
- Students and parent/guardian 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.
- Files stored on ~~District-managed networks~~ District Technology Resources are the property of the ~~school-district~~ District and, as such, may be inspected at any time and should not be considered private.

Instruction

Instructional Resources

STUDENT INTERNET USE (continued)

6417

- Materials published for electronic publication must be for educational purposes. School administrators, teachers and staff may monitor these materials to ensure compliance with content standards.

Fairfield Public Schools reserves the right to refuse access to the Internet to District Technology Resources to anyone any student. Violating any portion of this policy, District and/or administrative policies, rules or regulations, or state or federal laws may result in disciplinary action, including temporary or permanent ban on computer or Internet use student use of District Technology Resources and/or use of personal electronic devices on school property or during school sponsored activities, suspension or dismissal from school and/or legal action. The District will cooperate with law enforcement officers in investigations related to illegal activities conducted through its network with District Technology Resources or personal electronic devices.

District Technology Resources include but are not limited to District owned, operated, managed or offered electronic media information, devices, resources, systems; software, hardware and programs; networks and access to the internet; cell phones, smart phones, tablets (Kindles, Nooks, IPads etc.), personal laptop and desktop computers, memory sticks, or any device or item that can or may be capable of receiving, transmitting and/or storing digital information or digital media.

Personal electronic devices include, but are not limited to: cell phones, smart phones, tablets (Kindles, Nooks, IPads etc.), personal laptop computers, memory sticks, or any device or item that can or may be capable of receiving, transmitting and/or storing digital information or digital media.

Legal Reference: Connecticut General Statutes 53a-182b Harassment in the first degree: class d felony (as amended by PA 95-143)

Legal Reference: RSA 194:3-d, 47U.S.C. Section 254, Children's Internet Protection Act.

CREF 6417

Approved 8/27/04

Fairfield Board of Education
Fairfield, Connecticut

NOTICE

ELECTRONIC MONITORING

4235

This policy also serves as the required posting notice.

Pursuant to the authority of Public Act 98-142, the Board of Education hereby gives notice to all its employees of the potential use of electronic monitoring in its workplace. While the Board may not actually engage in the use of electronic monitoring, it reserves the right to do so when determined to be appropriate by the Board or the Superintendent of Schools at their discretion.

“Electronic monitoring,” as defined by Public Act 98-142, means the collection of information on school district premises concerning employees’ activities or communications, by any means other than direct observation of the employees. Electronic monitoring includes the use of a computer, telephone, wire, radio, camera, electromagnetic, photo-electronic, or photo-optical systems. The law does not cover the collection of information (A) for security purposes in any common areas of the Board of Education premises which are open to the public, or (B) which is prohibited under other state or federal law.

All staff members are made aware of the following:

- Virtually, all electronic devices retain a record of each use and the information about that use may be recoverable.
- Electronic communications may not be secure and therefore may not be an appropriate means by which to communicate confidential or sensitive information.
- Freedom of Information Regulations apply to information maintained and/or communicated electronically **as well as and** to information maintained or communicated on other media.

The following specific types of electronic monitoring may be used by the school district in its facilities:

- Monitoring of e-mail and other components of the school district’s computer system for compliance with policies.
- Video surveillance **of employee parking areas in school buildings and on school grounds except where prohibited by law** for security purposes.
- **Video surveillance on all school transportation vehicles.**
- Telephone monitoring **(office, professional calls only) (landlines, cell or wireless)** for quality control and performance assessment.
- Monitoring of electromagnetic card access system for security purposes.

ELECTRONIC MONITORING (continued)

4235

The law also provides that, where electronic monitoring may produce evidence of misconduct, the school district may use electronic monitoring without prior notice when the Board and/or Superintendent have reasonable grounds to believe employees of the school system are engaged in conduct that (1) violates the law or professional codes of conduct, (2) violates the legal rights of the Board of Education or other employees, (3) creates a hostile work environment, or (4) violates Board policy or regulations.

Questions about electronic monitoring in the workplace should be directed to the Superintendent of Schools or members of the administrative staff.

Approved 8/27/04