Instruction

Computers: Responsible Computer, Network and Internet Use

Overview

The Sterling Board of Education (Board) provides its students and staff access to a multitude of technology resources. Access to information and communication technologies (ICT) is considered a privilege and not a right. ICT resources consist of any technology and/or devices that access or convey information, software applications, Internet resources and Internet environments; including cloud-based solutions.

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. The District also makes a good faith effort to protect its students from exposure to Internet materials that are harmful or explicit. The District maintains a system of Internet content filtering devices and software controls that meet federal standards established in the Children's Internet Protection Act (CIPA).

Digital Citizen

The District uses information and technology in safe, legal, and responsible ways. It is incumbent upon all members of the school community to use technology ethically, constructively, and with respect for the work of others. Independent and appropriate use of information and communication technologies is predicated upon responsible and ethical conduct. Therefore, a responsible digital citizen, whether staff, student or volunteer, is one who:

• **Respects One's Self.** Users will select online names that are appropriate and honest about one's identity, and will consider the information and images that are posted online. Users will communicate and interact with others in respectful ways.

• **Respects Others.** Users will refrain from using technologies to bully, tease or harass other people. Users will not access or use hate-based or sexually explicit materials nor will they disparage others.

• **Protects One's Self and Others.** Users will protect themselves and others by reporting abuse and not forwarding inappropriate materials or communications. Users will adhere to age requirements and guidelines of all websites. Users will protect personal information and respect the privacy of others' information.

• **Respects Intellectual Property.** Users will suitably cite any and all use of websites, books, media, etc.

• **Protects Intellectual Property.** Users will request to use the software and media others produce. Respect will be shown for intellect and creativity by asking permission, giving credit and observing the law.

• **Respects Classroom Guidelines.** Users will follow all guidelines set by teachers regarding the use of electronic devices. Users will respect teachers by keeping all communication school related.

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 compute user (staff and students) will be required to read the responsibility use policy and to sign the responsible use agreement. 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.

• 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.

• 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.

Communications via ICT resources are often public in nature and general school rules and communication apply. It is expected that users will at all times comply with District standards and will act in a responsible and legal manner in accordance with District standards as well as with federal and state laws.

It is important that all users and parents understand that the District, as owner of the ICT resources, reserves the right to monitor and review the use of ICT resources. Such monitoring or review will be limited and done, as needed to ensure that the systems are being used for District-related educational purposes. Therefore, all users must be aware that they should not have any expectation of personal privacy in the use of these ICT resources.

Monitoring access is for, but not limited to, the following reasons:

• Ensuring the safety and security of people and resources;
• Ensuring positive learning and work environments;

- Keeping schools safe from harassment, intimidation or threats;
- Ensuring ICT resources use relates to educational mission and goals;
- Preventing breaches of confidentiality;
- Prevention of copyright infringements;
- Ensuring appropriate Internet access;
- Ensuring appropriate communication messages, such as email, blogs, chats and discussion forums; and
- Ensuring appropriate file downloads and print requests.

Policy Violations

The District reserves the right to refuse access to the Internet to anyone. Violating any portion of this policy may result in disciplinary action, including temporary or permanent ban on computer or Internet use, suspension or dismissal from school, and/or legal action. The District may cooperate with law enforcement officers in investigations related to illegal activities conducted through its network.

Legal Reference: Connecticut General Statutes

> 53a-182b Harassment in the first degree: Class D felony. (as amended by PA 95-143)
>
> 20 U.S.C. Section 6777, No Child Left Behind Act
>
> 20 U.S.C. 254 Children's Internet Protection Act of 2000
>
> 47 U.S.C. Children's Online Protection Act of 1998
>
> Public Law 110-385 Broadband Data Improvement Act/Protecting Children in the 21st Century Act

Policy adopted: March 19, 2013