Seekonk Public Schools
Technology Acceptable Use and Internet Safety Policy
Administrative Procedure

Purpose
The purpose of the Seekonk Public Schools Computer Acceptable Use and Internet Safety Policy is to promote use of district technology for educational purposes, to prevent inappropriate use of district technology, to prevent breaches of network security, and to comply with federal and state regulations. A user is defined as any employee, student, or guest (community member, visiting teacher, etc.) using technology in the Seekonk Public Schools. Technology includes any and all equipment, software, and materials that provide access to the district network and computer resources and the Internet. This document provides information about the users' responsibility to safeguard technology equipment and information from accidental or deliberate unauthorized access, tampering, snooping, distribution, or destruction. It sets forth what is, and is not, appropriate use of school district technology. Users will be disciplined for noncompliance in accordance with school district disciplinary policies. This policy does not purport to address every acceptable or non-acceptable technology use issue. It is your responsibility to use sound judgment. Should you identify an issue or situation that you are not certain how to deal with, inquire of your teacher, the building administrators or the Technology Department. The school district may add to, or change, this procedure at any time. The ***Seekonk Public Schools Contract for Access to Technology Resources*** forms must be signed yearly by staff and students. Users under the age of 18 must also have a parent or guardian sign the form. Signed forms shall be returned to the building administration for record keeping purposes. Copies of this procedure as well as the policy and forms will be available in every building office as well as on the Seekonk Public Schools' website at <http://www.seekonkschools.org>.

The first, best, and most important line of defense starts with our staff and students!

User Responsibilities
Users are responsible for the appropriate use of school district computers and other technology, and for taking reasonable precautions to secure the information and equipment entrusted to them in accordance with school district policies and practices. Users are responsible for reporting inappropriate use of school district technology, and breaches of computer/network security. The building administrator is responsible for ensuring compliance with this policy in his/her building. Students are prohibited from having liquids and other food items while utilizing district technology. Violations of the Acceptable Use Policy that may constitute a criminal offense may be referred to law enforcement authorities.

Unauthorized Access/Damage to Equipment
Any form of tampering, including snooping and hacking, unauthorized access, or destruction, theft or alteration of district technology equipment, data, and/or materials is a violation of school district policy, and will be investigated with appropriate disciplinary action taken.

Password Protection
Passwords are confidential. All passwords shall be protected by the user and not shared or displayed. Staff passwords expire once a year and must be changed. Student passwords are assigned and are available to staff members in the student's school. To request a change in a password, a student should make a request to their building administrator(s). Users shall not use another user's account.

Handling Confidential Information
All electronic information is considered confidential unless you have received permission to use it. Accessing or attempting to access confidential data is strictly prohibited. Confidential information should only be used for its intended purpose. Using confidential information for anything other than its intended use is prohibited, without prior administration approval. No confidential information shall be posted to a public web site.

Laptops and other Mobile Technology
The following are measures that should be taken when utilizing mobile technology owned by the district:

- Report damaged, lost, or stolen devices immediately
- Use reasonable precautions to safeguard the device against accidental damage, loss, or theft.

Copyright Infringement
All school district software shall only be used in accordance with the terms of the software licensing agreements. Unauthorized copying, redistributing, and republishing of copyrighted or proprietary material is strictly prohibited. In general, all information accessible via the Internet should be assumed to be private property. Users are responsible for citing Internet sources and giving credit to authors. If you have questions about copyright infringement, discuss it with the administration immediately.

Harassment, Threats and Discrimination
It is school district policy, and the law, that users are able to work free of unlawful harassment, threats, and discrimination. Any use of school district technology for cyber bullying, harassment, threats, or discrimination is strictly prohibited. All incidents of cyber bullying shall be reported in accordance with the district anti-bullying policy.

Changes to School District Computers
Installing software and making changes to technology hardware, software, system configuration, and the like are prohibited, without the Technology Department's authorization.

Personal Use of Computers
Personal use of district technology by employees is permitted for reasonable activities that do not need substantial technology resources. Use of school district technology for illegal or unethical purposes is prohibited.

Privacy - Monitoring Computer Communications and Systems
The school district reserves the right, without prior notice, to log, monitor, access, disclose, use, review, or remove both school and personal computer communications (including email, chat rooms, instant messaging, and on-line activities) and information, and will do so for legitimate district purposes. The school district will investigate complaints about inappropriate images on computers, inappropriate e-mail, or other inappropriate conduct. The school district makes every effort to monitor student Internet activity in accordance with the Children's Internet Protection Act (CIPA). All information and data contained on district networks and technology resources is considered district property.

Internet Safety
Use of the Internet is not without potential dangers. Users must follow established computer operating policies and practices to reduce the opportunity for security breaches, and inappropriate or illegal activity resulting from connecting to the Internet. Seekonk Public Schools, as part of our curriculum, provides education to students as appropriate through all grade levels on online safety including cyber bullying and online interactions.

In accordance with the CIPA, the Seekonk Public Schools has installed filters that block or filter Internet sites that are obscene, contain pornography, or contain material that is deemed locally to be inappropriate or harmful to minors. Staff members that believe that an Internet site has been incorrectly blocked may submit, in writing or via email, a request to the Technology Department to unblock the site. Any student or staff member that has unintentionally accessed an inappropriate site should report the site to their teacher/administrator. The teacher/administrator should then submit a request to the Technology Department to block the site.

Student Access to Computers and the Internet
Students have the responsibility to use computer resources for academic purposes. Students at all grade levels shall be supervised when using school district computers. Only those students whose parents have consented to technology use and Internet access will be allowed access to district technology and the Internet. Students shall demonstrate personal responsibility by agreeing not to meet with someone they contact online without first checking with parents.

Students providing support to the district may have access to administrative privileges not normally granted to students. These students are responsible for maintaining the security and integrity of any privileges that they have been granted access to.

School District employees are responsible for monitoring and supervising the use of computers and Internet access by students in their classrooms and/or offices.

Internet Connections
Internet connections are authorized for educational needs. Incidental and occasional use of the Internet for personal purposes by school district employees is permitted. The Internet should be considered a public forum for all transmissions. As such, no Internet communications or postings can be considered to be private.
The following actions are prohibited under any circumstances:

- Portraying yourself as someone other than who you are, or the school district you represent
- Accessing inappropriate web sites, data, pictures, jokes, files, and games
- Inappropriate chatting, e-mail, monitoring, or viewing
- Harassing, discriminating, or in any way making defamatory comments
- Transmitting junk mail, chain letters, or soliciting for commercial, religious, charitable, or political causes
- Gambling or any other activity that is illegal, violates school district policy, or is contrary to the school district's interests
- Students are not allowed to download any programs or to download any files not relating to their schoolwork.
- All users are prohibited from downloading unapproved programs.
- Students are not allowed to access online accounts other than e-mail. Students are allowed to access online accounts such as Google Apps and other web 2.0 tools that are related to their schoolwork. Students will not post personal information about themselves or other people on the Internet.
- Participating in types of use that the user knows or has reason to know would cause congestion on the network or interfere with the work of others

The school district, and the law, can and will hold you responsible for offensive, discriminatory, and defamatory statements, or any other illegal activity.

E-mail - Electronic Communications
District e-mail shall be used by staff for all school related e-mail correspondence. All staff e-mail is archived for 7 years and is considered property of the school district. Incidental or occasional use of e-mail for personal reasons is permitted. Students will only be assigned email accounts as needed for class work. Users are required to report inappropriate use of e-mail.

The following e-mail activity is prohibited:

- Discussing highly sensitive or confidential school department information
- Accessing, or trying to access, another user's e-mail account
- Using e-mail to harass, discriminate, or make defamatory comments
- Using e-mail to send inappropriate e-mail to third parties
- Transmitting school district records within, or outside, the school district without authorization
- Transmitting junk mail, chain letters, or soliciting for commercial, religious, charitable, or political causes
- Transmitting information that user knows or has reason to know would cause network congestion or harm to another user's data

Local Area Network (LAN)
All important, confidential, or proprietary information should be stored on the LAN. The LAN is equipped with additional electronic and physical security. All school district policies apply to the LAN. The following activities are prohibited, without Technology Department authorization:

- Installation of business or personal software on the LAN
- Making any changes to the LAN hardware or software
- Accessing without authorization LAN programs, data, and files
- Assisting anyone within, or outside, the school district in obtaining unauthorized access to the LAN

Use of Web 2.0 Tools

Uses of Web 2.0 Tools such as blogs, podcasts, and other online applications are considered a resource in support of our instructional and administrative programs. Guidelines for appropriate use of district technology resources extend to the use of Web 2.0 Tools. In addition, district rights, such as access and logging, to network resources extend to Web 2.0 Tools. By signing the appropriate Student Contract, parents are agreeing to allow their child permission to access these resources.

Responsibilities for Guest Users and Devices

Guest users are defined as users accessing the Internet through the district's networks for short-term uses such as workshops or presentations. These guests may utilize district technology devices or may provide their own device. The district host/hosts for these users is/are responsible for ensuring that the guest users are aware of and comply with district policies. No guest access is provided for district network resources other than the Internet. All guest access is filtered at the student level unless otherwise requested through the Technology Department. Guests that act as substitutes for staff or that need access on a recurring basis shall be regarded as staff members and must sign the Employee Contract for Access. Access to network resources shall be provided for long-term substitutes and other long-term guests upon written request to the Technology Department.

Guest devices are those devices that are brought into the district, but not owned by the district. Access to the district's networks for guest devices must be approved through the building administration and/or the Technology Department. These devices may be required to meet minimum requirements specified by the Technology Department. (For example, anti-virus and antispyware software installed.) Only staff and student devices utilized for educational purposes will be allowed on the district's networks.

Reporting Policy Violations
Users are required to report violations of the acceptable use policy immediately to your building administrator and/or the Technology Department. Noncompliance with the school district's acceptable use policy may result in discipline up to, and including, permanent denial of access to computer use and the requirement that the violator provide restitution. Users that report violations will be protected from discrimination, harassment, and any other form of retaliation.

Consequences of Violations
If a user is found in violation of this policy, the consequences imposed could be actions up to and including the following:

- Suspension or revocation of network privileges either temporarily or permanently
- Suspension or revocation of computer access privileges either temporarily or permanently
- Suspension or expulsion (students)
- Termination (staff)
- Notification of appropriate law enforcement agencies of suspected illegal activities. The district will cooperate fully with local, state, and/or federal officials in any investigation related to suspected illegal activities.
- Requirement that violator provide restitution for any loss or damages.

Student penalties shall be in accordance with school discipline policies.

This following forms support this procedure:

Seekonk Public Schools Contract for Access to Technology Resources - Individual Employees

Seekonk Public Schools Contract for Individual Student Access to Technology Resources - Middle School Students and High School Students

Seekonk Public Schools Contract for Individual Student Access to Technology Resources - Elementary School Students