Approved by the
Seekonk School Committee
August 26, 2002

Seekonk Public Schools
Computer Acceptable Use and Internet Safety Policy

Purpose

The purpose of the Seekonk Public Schools Computer Acceptable Use and Internet Safety Policy is to promote use of the Seekonk Technology Network for educational purposes, to prevent inappropriate use of district computers and breaches of computer security, and to comply with the Children's Internet Protection Act. A user is defined as any employee, student or guest (community member, visiting teacher, etc.) using a computer in the Seekonk Public Schools. This policy provides information about the computer users' responsibility to safeguard computer 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 computers. 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 computer 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 Network Administrator. The school district may add to, or change, this policy at any time. At the end of this policy are the ***Seekonk Public Schools Contract for Access to Computers, the Internet, and School-based Networks*** forms. The appropriate form must be signed yearly by students and other community users and guests. Users under the age of 18 must also have a parent or guardian sign the form. School District employees must sign the appropriate form when hired and whenever changes are made to this policy. The signed form should be given to the building administration for record keeping purposes. Copies of this policy will be available in every building office as well as on the Seekonk Public Schools' website at <http://www.seekonk.k12.ma.us>.

Introduction

The impact of the computer on education has been significant, and at breakneck speed. The technology accessible today could not have been speculated just five or ten years ago. Implementing new technologies is expensive, time consuming, and without established policies and practices in place, could lead to disaster.

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

For this reason, the District has created this Computer Acceptable Use and Internet Safety Policy. Please understand it is not our intention to encumber your use of the computer, but rather our fiduciary responsibility to protect the resources of the school district. We believe this policy accomplishes that with little or no hardship to you, the computer user.

Computer Acceptable Use Policy

Computer User Responsibilities
Computer users are responsible for the appropriate use of school district computers and for taking reasonable precautions to secure the information and equipment entrusted to them. Users are responsible for reporting inappropriate use of school district computers, and breaches of computer security. Users are responsible for adhering to school district policies and practices as described herein, and in other school district policy manuals and student handbooks. Users are responsible for ensuring school district computers are used in accordance with school district policy guidelines, and reasonable measures are taken to prevent loss or damage of computer information and equipment. The building administrator is responsible for ensuring compliance with this policy in his/her building.

Violations of the Acceptable Use Policy that may constitute a criminal offense may be referred to law enforcement authorities.

Unauthorized Access
Unauthorized access of school district computers is prohibited. Unauthorized access of third-party computers, using school district computers, is prohibited. Attempting to access school district computers without specific authorization is prohibited. Any form of tampering, including snooping and hacking, to gain access to computers is a violation of school district policy, and carries serious consequences. In addition, computer users must take reasonable precautions to prevent unauthorized access of school district computers.

Computer Sabotage
Destruction, theft, alteration, or any other form of sabotage of school district computers, programs, files, or data is prohibited and will be investigated and appropriate disciplinary action taken.

Password Selection and Protection
Select difficult passwords when applicable. Protect them from snoopers. A lot of damage can be done if someone gets your password. Novell network passwords will automatically expire once a year. Do not share your password with anyone, other than a designated school district administrator or network administrator. Do not write it down where someone can find it, do not send it over the Internet, Intranet, e-mail, or any other communication line. Do not leave a computer logged on when you leave it. Do not log on to a computer if someone can see you keying in your password (there is no need to create the temptation). Turn off computers at night. If you have a question about password selection or safekeeping, please see your Network Administrator. If you suspect that someone has discovered your password, notify the Network Administrator immediately.

Poor password selection and safekeeping <u>is not an acceptable excuse if anyone damages school district computer systems using your login name and password.</u>

Password Cracking
It is not uncommon for users to try to figure out a friend's, or associate's, password, just to see if they can. Stay away from such activity. It is a serious violation of school district policy.

Easy to Remember and Hard to Crack
Another concern is forgetting your password. A good method to help you remember your password is to select passwords that are unique to you, and try to use it at least once every day.
The following is a good guideline for password selection:

- Use 5 or more characters, and at least one alphanumeric character
- Your password should not include your login name, your name, a family member's name, or a pet's name, or any other names commonly known to others
- Your password should not be a word pertaining to the school district, your work, or an activity that you participate in or follow that is commonly known
- Your password should not include anything derogatory, offensive, or defamatory

Snooping
Exploring ways to access school district computer systems is a serious violation of school district policy. If you have no business being there, don't go there. If you accidentally identify a new way to access information, report it to the Network Administrator, a staff member (if a student) or the building administrator. Watching other users enter information, and looking at computer disks that do not belong to you, are prohibited. Obtaining, or trying to obtain, other users' passwords, or using programs that compromise security in any way, are violations of school district policy. If you observe someone snooping, report it immediately to the Network Administrator or appropriate staff member.

Hackers
It takes a concerted effort by all users to maintain secure computer systems. Hackers are working hard to break into computer systems. They alter and delete files, and cause other havoc for fun or profit. A common exposition of hackers prosecuted for criminal activity is that they felt computer systems' weaknesses exist to be exploited. Never give any information about computer systems out over the telephone, or in any other way. If someone requests such information, refer him or her to the Network Administrator or your building administrator.

Using hacker programs and trying to access computer systems using hacker techniques is prohibited. Trying to hack into third party computer systems using school district computers is prohibited, and may be reported to the local authorities. Hacker crimes result in millions of dollars of downtime, lost data, and other problems. If you are caught hacking, it is a serious offense. If you identify vulnerability in the school district's computer security system, report it to administration and the Network Administrator.

Viruses, Worms and Trojan horses
Diskettes are still the most common route of infection. However, e-mail and the Internet are rapidly growing sources of viruses. It is critical that users make certain that data and software installed on school district computers are free of viruses. Data and software that have been exposed to any computer, other than school district computers, should be scanned before installation. Never open email attachments from people you don't know (a virus can quickly contaminate your computer simply by opening an e-mail attachment). If using GroupWise, use the view attachment capability instead of opening attachments. Immediately delete any suspect email without viewing or opening. Viruses can result in significant damage, and lost productivity. If you are uncertain whether data or software needs to be scanned before installation, see the Network Administrator or their designee.

Use of virus, worm, or trojan horse programs is prohibited. If you identify a virus, worm, or trojan horse, or what you suspect to be one, do not try to fix the problem. Immediately turn your computer off, make notes as to what you observed, and contact the Network Administrator. The principal concern is stopping the contamination before additional damage is done. These programs are most successful when ignored. They are designed to easily hop from application to application, contaminate a computer disk, and access another computer. The key to containment is limiting the reach of the contamination. Turning off your computer best does this.

Handling Confidential Information

All computer 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.

It is important that users take extra care with confidential information stored on computers. The following are inappropriate under normal circumstances when dealing with confidential information:

- Printing to a printer in an unsecured area where documents may be read by others
- Leaving your computer unattended with confidential files logged on to your system
- Leaving computer disks with confidential data unattended, in easy to access places.
- Sending confidential information over the Internet, Intranet, dial-up modem lines, or other unsecured communication lines without approval from the administration

If you observe a document at a shared printer, or any other location, do not read it without permission.

Encryption

Encryption and encryption utilities are prohibited without Network Administration approval. If you need to send confidential or proprietary information over the Internet, or other public communication lines, you must ascertain that the transmission is secure.

Physical Security

Physical security is key to protecting your computer and computer information from loss and damage. Store floppy disks and other sensitive information in a locked drawer. Turn off your computer when it is not in use for an extended period of time. Employees should lock the door to their classroom or office when they leave. Laptops should be placed in a secure place and not left on a desk. Take a few minutes to practice good physical security. Your investment of time will provide an excellent return, and help prevent temptation by others.

Laptops

There is no sure way to secure laptops. However, there are many sensible, cost-effective measures that can help reduce the risk of loss or damage. The following are required when taking laptops off school district property:

- Report lost or stolen computers immediately
- Use reasonable precautions to safeguard the laptop against accidental damage (example - don’t work on your laptop in the pool)

- Use reasonable precautions to safeguard the laptop against theft (example - don't leave the laptop in plain view in an unlocked car)
- When traveling, laptops must be in sight at all times or physically secure

Back-up
The Seekonk Public Schools will not be responsible for regular back up of computer files not stored on servers. All important proprietary information should be stored on the local area network (LAN). Maintenance and back up are performed on the LAN regularly. Programs and other information are updated on the LAN regularly. Use the LAN, it is safe, effective, and reliable.

Copyright Infringement
The school district does not own computer software, but rather licenses the right to use software. Accordingly, school district licensed software may only be reproduced by the Network Administrators or their designees in accordance with the terms of the software licensing agreements. Unauthorized copying, redistributing, and republishing of copyrighted or proprietary material is strictly prohibited. Copyright laws apply on the Internet as well. There is no "but copying it was so easy" defense to copyright infringement. Copyright infringement is serious business, and the school district strictly prohibits any such activity. 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.

All programs including shareware or "free" programs must be approved for installation by the Network Administrator. Shareware and free software often have licensing and use restrictions, and should not be copied or forwarded to others. Typically, if you continue to use shareware you must send in a "donation," often of a specified amount. If you neglect to do so, you may have committed copyright infringement. If you provide the program to a friend, you may have violated copyright law. It is not unusual for "free" software to contain a virus. As such, it is important that all new software, including applications are approved by the Network Administrator.

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. Unlawful harassment is physical or verbal behavior directed towards an individual due to their race, age, marital status, gender, disability, religion, sexual orientation, or nationality for the purpose of interfering with an individual's work performance, or creating an intimidating or hostile work environment.

It is not uncommon for users to receive files, data, pictures, games, jokes, etc. that may be considered offensive by some. Currently, there are many cases in the courts addressing just such issues, the ramifications of which are significant. The computer is possibly the easiest tool for obtaining, storing, sharing, and disseminating to large audiences such material and viewpoints. Stay away from such activity; it is a serious violation of school district policy.

Computers provide a huge potential for unlawful harassment. Users often think their communications are private, and trashed or deleted files are gone forever. However, deleted files are often easily recovered; and information on school district computers is not necessarily private. Remember,

whatever you transmit is a permanent record to the receiver. It can, at some future date, be taken out of context and used against you and the school district.

Accidents, Mistakes and Spills

"An ounce of prevention is worth a pound of cure" is a very appropriate cliché for computer operations. Take a few seconds to read the computer screen before you delete, save, or transmit files. In addition, users need to take reasonable precautions with respect to computer operations, maintenance, handling, and transportation. Students are prohibited from having liquids and other food items at computers.

Changes to School District Computers

Installing software and making changes to computer hardware, software, system configuration, and the like are prohibited, without the Network Administrator's authorization. The school district's computer systems have been designed and documented to prevent loss of data, and provide an audit trail for correcting problems. Unauthorized changes to computer systems ultimately result in lost productivity. Such changes often require a computer technician to fix both the original problem, and the problem caused by the would-be computer technician. Poor documentation of the procedures performed, and the order in which they were completed further complicate unauthorized changes to computer systems.

The following are just a few examples of changes to computers that can result in operating problems:

- Installation of commercial software, shareware, and free software. Some software requires an upgrade of computer hardware, the operating system, or both for the program to operate properly. Some programs are simply not written well, and can cause problems with the computer
- Installation of some programs changes the computer's system configuration, which can result in problems with your computer and with access to the network
- Data used on home computers may become infected with a virus, and contaminate your computer and other school district computers

The list of potential problems goes on and on. Accordingly, get approval from the Network Administrator before making any changes to school district computers.

Personal Use of Computers

Personal use of school district computers by school district employees is permitted for reasonable activities that do not need substantial computer hard disk space, or other computer equipment. Use of school district assets for personal gain or benefit is prohibited. Prohibited activities include, but are not limited to personal software and hardware, and running a personal business on the side. Using school district computers to store or transmit inappropriate jokes, junk mail, chain letters, or to solicit for commercial, religious, charitable, or political causes is prohibited. If you are uncertain about a specific activity, ask your building administrator. Personal files, information, and use of school district computers will be treated no differently by the school district than school use, with regard to employee privacy.

Many software games and some shareware programs are illegally copied, and often contain viruses. Such programs represent a potential liability to you and the school district. Proof of ownership and Network Administrator authorization for installation/use is required for all software on school district

computers. Coming to work with a computer program, on an unlabeled disk, you received from a friend of a friend is prohibited.

Reporting Policy Violations
Users are required to report violations of computer policy. Violations should immediately be reported to your building administrator and the Network Administrator. Noncompliance with the school district's computer 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. Hackers, snoopers, password stealers, virus installers, data deleters, and anyone involved in such activity will be disciplined. If you identify a computer security vulnerability, you are required to report it immediately to the Network Administrator.

Privacy - Monitoring Computer Communications and Systems
The school district reserves the right, without prior notice, to monitor, access, disclose, use, 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. Random audits to verify that school district computers are clear of viruses, and used in accordance with school district policy, may be performed. The school district will investigate complaints about inappropriate images on computers, inappropriate e-mail, or other inappropriate conduct. The school district may monitor Internet activity to see what sites are frequented, duration of time spent, files downloaded, and information exchanged. Again, computer systems and information are school district property, and should be used principally for education purposes.

External Communications - Third Parties
The same standards of decorum, respect, and professionalism that guide us in the school environment apply to computer communications with third parties.

Internet Safety
Use of the Internet is not without potential dangers. Copyright laws can be enforced on the Internet. Viruses can be downloaded from the Internet. Inappropriate web sites, images, and communications exist on the Internet. Hackers exist on the Internet. As such, 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.

In accordance with the Children's Internet Protection Act, the Seekonk Public Schools has installed firewalls 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, a request to the Network Administrator 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 Network Administrator to block the site.

The Seekonk Public Schools reserves the right to monitor all use of the school networks including but not limited to email, chat rooms, electronic communications such as instant messaging, and on-line activities. In addition, use of chat rooms and electronic communications such as instant

messaging by students is prohibited unless as authorized by the Network Administrator and building administrator for classroom use.

Any student or staff member should immediately tell their teacher/administrator if they receive a message that is inappropriate or makes them feel uncomfortable.

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 Internet access will be allowed Internet access. Students shall demonstrate personal responsibility by agreeing not to meet with someone they contact online without first checking with parents. Students are not allowed at any time to enter or participate in a chat room. Students are not allowed to access personal Internet or communication accounts (such as instant messaging) from school. Students will not post personal information about themselves or other people on the Internet. District employees may distribute personal student information only after obtaining a ***Photograph and Sound Release Form*** signed by the student's parent or guardian. However, the following student information should never be posted: last names, addresses, phone numbers,ages or birthdates, parent's names, or any pictures with names.

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. Individuals connecting to the Internet should understand that such transmissions are identifiable and attributable to the school district. Disclaimers such as "***The opinions expressed do not necessarily represent those of the school district,***" while a good idea, do not necessarily relieve the school district of liability. The Internet should be considered a public forum for <u>all</u> transmissions. As such, no Internet communications or postings can be considered to be private. All communications on the Internet provide an opportunity for a permanent record, and can be edited and retransmitted. Accordingly, maintain decorum in all communications and transmissions.
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 (such as AOL) or to access chat rooms, bulletin boards, or instant messaging services. Students are not allowed to post to or create websites unless related to their schoolwork.
- 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

Please keep in mind, a statement or posting of information on the Internet can cause serious damage, because information can be quickly and effectively disseminated. 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

E-mail is a wonderful tool. Used correctly, it can provide significant efficiencies, and improve the quality of the way we do business. It makes dissemination of information easy and cost-effective. Please take full advantage of it.

The same standards of decorum, respect, and professionalism that guide us in our face-to-face interactions apply to the use of e-mail. Incidental or occasional use of e-mail for personal reasons is permitted. Students will only be assigned email accounts as needed for class work.

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
- Obtaining, or distributing, another user's e-mail account
- Using e-mail to harass, discriminate, or make defamatory comments
- Using e-mail to make off-color jokes, or 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

Users are required to report inappropriate use of e-mail.

Local Area Network

All important, confidential, or proprietary information should be stored on the LAN. The LAN is equipped with electronic and physical security. Activity on the network is monitored for tampering and other security breaches. Maintenance and back-up are performed on the LAN regularly; and programs and other information are updated regularly. Use the LAN! It is safe, effective, and reliable. All school district policies apply to the LAN. The following activities are prohibited, without Network Administrator 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

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.

List of Forms

This list of forms are considered to be a part of this policy:

Seekonk Public Schools Contract for Access to Computers, the Internet, and School-based Networks Individual Employees and Guests

Seekonk Public Schools Contract for Individual Student Access to Computers, the Internet, and School-based Networks - Middle School Students and High School Students

Seekonk Public Schools Contract for Individual Student Access to Computers, the Internet, and School-based Networks Elementary School Students

Seekonk Public Schools Contract for
Access to Computers, the Internet, and School-based Networks
Individual Employees and Guests

I have received and read the school district's Computer Acceptable Use and Internet Safety Policy and this Contract for Access to Computers, the Internet, and School-based Networks. I understand that I am responsible for adhering to and abiding by the policies and practices described in the Seekonk Public Schools Computer Acceptable Use and Internet Safety Policy (AUISP). I understand that a full copy of the AUISP is available in any school building or on the schools' website at <http://www.seekonk.k12.ma.us>. I understand that this AUISP may be added to, or changed by the school district at any time.

It is my responsibility to:

- Bring any questions I have about the AUISP to the building or district Administration.
- Report any violations of this policy that I witness, or become aware of.
- Respect all copyrights and software licensing.
- Supervise any students using computers under my care.
- Safeguard computer equipment and information from accidental or deliberate unauthorized access, tampering, snooping, distribution, or destruction.

Further, I understand that:

- I must not install software or change system settings without authorization from the Network Administrator.
- I must not install software on more computers than the software license allows.
- I may use school district's computers for personal use as long as it does not require excessive hard disk space or other computer resources and is not for personal gain or benefit.
- All school district computers and network equipment including electronic mail messages that I transmit and receive, cached files and other files are school district property, not personal property, and as such can be accessed, disclosed, removed, or monitored at any time. Also that Internet access may be blocked to certain sites.
- Should I commit any violation of the Seekonk Public Schools AUISP, my access privileges will be revoked and school disciplinary action or appropriate legal action may be taken.

I agree to indemnify the Seekonk Public Schools for any losses, costs or damages, including reasonable attorney's fees, incurred by the Seekonk Public Schools relating to or arising out of any intentional violation by me of this Agreement.

_____ _____

Employee Signature Date

_____ _____

Employee Name (please print) Building

Seekonk Public Schools Contract for Individual Student
Access to Computers, the Internet, and School-based Networks
Middle School Students and High School Students

The use of electronic resources (i.e. computers, school-based networks, etc.) and the Internet provides great educational benefits to students. Access to these electronic resources and the Internet is given as a privilege to students who agree to act in a considerate and responsible manner. Unfortunately, there are certain activities and some materials accessible via the Internet that are considered illegal, defamatory, or potentially dangerous to the integrity of the network and the safety of minors. Misuse of these materials and the subsequent loss of access to these privileges will certainly make the educational process difficult at best.

The purpose of the Seekonk Public Schools Computer Acceptable Use and Internet Safety Policy (AUISP) is to promote the use of the Seekonk Public Schools technology network for educational purposes,to prevent inappropriate use of district computers and breaches of computer security, and to promote safe use of the Internet. It is not the district's intention to encumber the use of the computer, but rather our fiduciary responsibility to protect the resources of the school district. The AUISP and this contract set forth what is, and is not, appropriate use of school district computers. However, they do not purport to address every acceptable or non-acceptable computer use issue. Seekonk Public Schools will make determinations on whether specific uses of electronic resources and the Internet are consistent with the intent of the AUISP and will periodically revise the policy on an as needed basis. A full copy of the AUISP is available at each school building and on the schools' website at <http://www.seekonk.k12.ma.us>.

Users will be disciplined for noncompliance in accordance with school district disciplinary policies. In addition, violations that may constitute a criminal offense may be reported to law enforcement authorities. Should you identify an issue or situation that you are not certain how to deal with, inquire of your teacher, the building administrator or the Network Administrator. We require that students and parents or guardians of minor students read, accept, and sign this contract at the beginning of each school year. This contract provides a partial summary of rules for acceptable behavior per the AUISP.

1. Students are responsible for good behavior when using electronic resources and the Internet just as they are in school. General school rules for behavior and communications apply. The access and use of your account must be consistent with the educational objectives of the Seekonk Public Schools.

2. Network storage areas as well as other electronic resources will be treated as school property; it is not considered to be personal property. This includes all cache files, electronic mail messages that any user sends or receives, and other files. Network administrators and designated staff of the Seekonk Public Schools may review and monitor files, communications, and other logs to maintain system integrity and to ensure that the system is being used responsibly. In addition, access to certain Internet sites may be blocked.

3. The following are prohibited:

    - The use of any electronic resources without the direct supervision of the staff of the Seekonk Public Schools
    - Downloading, sending or displaying offensive messages or pictures
    - Using obscene, profane or vulgar language
    - Harassing, threatening, insulting or attacking others, discriminatory remarks and any other antisocial behaviors
    - Transmitting or knowingly receiving any materials in violation of any United States or state copyright laws and regulations.
    - Using information from the Internet without properly crediting the author or without respecting copyrights.
    - Use of the network for commercial activities, product advertising, political advertising, or personal and private business
    - Accessing outside web site or E-mail or other communication accounts
    - Participating in chain letters, broadcasts, listservs, newsgroups, chat rooms or discussion groups without express prior permission

- Use of electronic resources for recreational gaming without the permission of the staff of the Seekonk Public Schools
- Using another's password or trespassing in another's folders, work, or files
- Allowing others to access your account or password
- Any material brought in from the outside (i.e. floppy disks, CD-ROMs, external peripherals) will not be used without clearance by the staff of the Seekonk Public Schools
- The downloading and/or installation of any programs onto the network or any computers. Downloading non-program materials (i.e. music files, images, text files) is done only by permission of the staff of the Seekonk Public Schools
- Intentionally wasting limited resources, including paper, ink, and network time.
- Vandalizing the system by harming or destroying the data or hardware on this system or any other system from this network.
- Posting of any personal information about any person
- Bringing of any drinks or other food items into the computer area
- Attempting to cause or intentionally causing congestion of the network or destruction of another user's data

4. You are expected to respect the integrity of electronic resources and the network by not intentionally developing or activating programs that infiltrate or alter the system software or hardware components. This includes but is not limited to viruses, hacking, or attempting to use administrative commands. Hardware or software shall not be destroyed, modified, or abused in any way

5. Security of the Seekonk Public Schools electronic resources is essential. Access to electronic resources is intended for the exclusive use of the authorized users who abide by this policy. Any problems that arise from the use of a network account are the responsibility of the account holder. All violations must be reported immediately to the staff of Seekonk Public Schools.

6. Violations of this contract and the AUISP will be investigated and appropriate disciplinary or legal action taken. Violations may result in suspension of network accounts and/or permanent or temporary loss of access to the network.

Use of the network will not be allowed until this policy is signed by both student and parent/guardian (for minor students) and returned to Seekonk Public Schools Administration.

Signature Page – Please sign and return to your school office.

I have received and read the ***Contract for Individual Student Access to Computers, the Internet, and School-based Networks***. I understand the rules, and agree to comply with the above stated rules and the Seekonk Public Schools AUISP. It is my responsibility to bring any questions I have about the AUISP to the building or district Administration. I further understand that, should I commit any violation, my access privileges may be revoked and school disciplinary action or appropriate legal action may be taken including reimbursement for damages.

Student Signature: _____ Date:_____

Student Name (please print): _____ School: _____

As the parent or guardian of this student, I have received and read the ***Contract for Individual Student Access to Computers, the Internet, and School-based Networks***. I have discussed the rules with my child. I understand a full version of the Seekonk Public Schools AUISP including this contract is available in each school or on the Seekonk Public Schools website at <http://www.seekonk.k12.ma.us>. I grant permission for the above student to access networked electronic resources, to receive a network account, and to access the Internet from school. I understand that this access is designed for educational purposes and that although precautions have been taken to eliminate controversial material, it is impossible to restrict access to all controversial material and I will not hold the Seekonk Public Schools responsible for materials acquired on the network. Further, I accept the responsibility for providing guidance to the above student on Internet use both inside and outside of the school setting, and for conveying standards for the above student to follow when selecting, sharing, or exploring information and media. I agree to indemnify the Seekonk Public Schools for any losses, costs or damages, including reasonable attorney's fees, incurred by the Seekonk Public Schools relating to or arising out of any violation of this Agreement.

Parent's Signature: _____ Date: _____

Seekonk Public Schools Contract for Individual Student Access to Computers, the Internet, and School-based Networks
Elementary School Students

The use of electronic resources (i.e. computers, school-based networks, etc.) and the Internet provides great educational benefits to students. Access to these electronic resources and the Internet is given as a privilege to students who agree to act in a considerate and responsible manner. Unfortunately, there are certain activities and some materials accessible via the Internet that are considered illegal, defamatory, or potentially dangerous to the integrity of the network or the safety of the student. Misuse of these materials and the subsequent loss of access to these privileges will certainly make the educational process difficult at best.

The purpose of the Seekonk Public Schools Computer Acceptable Use and Internet Safety Policy (AUISP) is to promote use of the Seekonk technology network for educational purposes to prevent inappropriate use of district computers and breaches of computer security, and to promote safe use of the Internet. It is not the district's intention to encumber the use of the computer, but rather our fiduciary responsibility to protect the resources of the school district. The AUISP and this contract set forth what is, and is not, appropriate use of school district computers. However, they do not purport to address every acceptable or non-acceptable computer use issue. Seekonk Public Schools will make determinations on whether specific uses of electronic resources and the Internet are consistent with the intent of the AUISP and will periodically revise the policy on an as needed basis. A full copy of the AUISP is available at each school building and on the schools' website at <http://www.seekonk.k12.ma.us>.

Users will be disciplined for violations of the computer AUISP in accordance with school district policies. We require that students and parents or guardians of minor students read, accept, and sign this contract at the beginning of each school year.

This contract provides a partial summary of rules for acceptable behavior per the AUISP for elementary age students and their parents as follows:

- I will only use the computer when my teacher gives me permission to and it is my turn.
- I will only use the computer to do the things my teacher has told me to do.
- I will not change settings on the computer.
- I will not do anything to break the computer or anything attached to the computer.
- I will not have food, drinks, or candy at the computer.
- I will only visit the Internet sites that my teacher has told me I can.
- I will not access my home email account or instant message account.
- I will not give out my name or picture or any personal information about myself or anyone else on the Internet.
- I will only download information from the Internet that my teacher has told me I can.
- I will not bring programs from home and put them on the computer.
- I will tell my teacher if I see anyone doing anything wrong on the computer.
- If I do not follow the rules, I will not be able to use the computer.

Signature Page – Please sign and return to your school office.

My teacher and my parent or guardian have discussed the rules for using computers in school. I agree to follow these rules. If I break these rules, I will not be able to use the computers. If I break the rules repeatedly, I may not be able to use computers in school for the rest of the year. If I have any questions or if I see anyone else doing something wrong, I will tell my teacher.

Student Signature: _____ Date:_____

Student Name (please print): _____ School: _____

As the parent or guardian of this student, I have received and read the ***Contract for Individual Student Access to Computers, the Internet, and School-based Networks***. I have discussed the rules with my child. I understand a full version of the Seekonk Public Schools AUISP including this contract is available in each school or on the Seekonk Public Schools website at <http://www.seekonk.k12.ma.us>. I grant permission for the above student to use school computers, to access networked electronic resources and to access the Internet from school. I understand that this access is designed for educational purposes and that although precautions have been taken to eliminate controversial material, it is impossible to restrict access to all controversial material and I will not hold the Seekonk Public Schools responsible for materials acquired on the network. Further, I accept the responsibility for providing guidance to the above student on Internet use both inside and outside of the school setting, and for conveying standards for the above student to follow when selecting, sharing, or exploring information and media and using computers. I agree to indemnify the Seekonk Public Schools for any losses, costs or damages, including reasonable attorney's fees, incurred by the Seekonk Public Schools relating to or arising out of any violation of this Agreement.

Parent's Signature: _____ Date: _____