Seekonk Public Schools
Technology Responsible Use and Internet Safety Policy

Purpose

The purpose of the Seekonk Public Schools Technology Responsible Use and Internet Safety Policy is to promote use of 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, volunteer, or guest (community member, visiting teacher, etc.) using technology in the Seekonk Public Schools or using technology off District property in a way that substantially and materially disrupts the school environment. Technology includes, but is not limited to, any equipment, software, and materials that provide access to the district network, computer resources and the Internet, and any electronic devices or computers, whether or not they utilize District resources. This document provides information about the user's 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 or technology on campus. The use of technology is a privilege and not a right. Users will be disciplined for noncompliance in accordance with school district disciplinary policies and may lose computer privileges. 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 eighteen (18) must also have a parent or guardian sign the form. 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://seekonk.sharpschool.com/>. All users are required and must remain up-to-date in their knowledge of the Policy, as updated.

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 technology on campus or inappropriate use of technology that substantially and materially disrupts the school environment, 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.

The Seekonk Public Schools provides access to its technology primarily for educational and administrative purposes. Approved uses include, but are not limited to, research, communication, and activities that support Seekonk Public Schools' educational mission.

Users may not utilize technology in a manner that would violate any federal, state, or local statute, rule, regulation or policy.

Unauthorized Access/Damage to Equipment

Any form of tampering, including snooping and hacking, unauthorized access, or destruction, theft or alteration of 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 (such as wifi, hardware passwords, student information system, TeacherPlus Gradebooks and Plus Portals, GAFE accounts, etc.) shall be protected from use by anyone other than the assigned user. Although the primary responsibility for passwords falls on students, staff members have the option to access student accounts and/or reset passwords when necessary.

Handling Confidential Information

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 or uploaded to Google Drive.

Users shall promptly notify the superintendent's office in the event that an e-mail transmission containing the confidential or proprietary information of another party is received without the express permission of that party.

Laptops and other Mobile Technology

The following are measures that should be taken when utilizing technology owned by the district:

- Report damaged, lost, or stolen devices immediately to your building administrator and the Technology Department.
- Use reasonable precautions to safeguard the device against accidental damage, loss, or theft.

Copyright Infringement

All software used on school grounds 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 concerns about copyright infringement, discuss it with the administration and/or your library media specialist 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 technology for cyberbullying, harassment, threats, or discrimination is strictly prohibited. All incidents of cyberbullying shall be reported in accordance with the district anti-bullying policy.

Users are expected to be polite and not abusive to other users, utilize appropriate language, such as no swearing, vulgarity or other inappropriate language, and consider what others may find hurtful or offensive when sharing content.

Changes to School District Computers

Installing software and/or making changes to such things as: hardware, software, system configuration or system settings are prohibited without the Technology Department's authorization. Infractions by users may be subject to disciplinary action.

Personal Use of Computers

Personal use of district technology by employees is permitted for reasonable activities that do not require 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 online activities) and information, and will do so for legitimate district purposes. No user shall have any expectation of privacy regarding such materials. The school district will investigate

complaints about inappropriate images on computers, inappropriate email, 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 such as cloud computing contained on district networks and technology resources is considered district property.

As public material, all information maintained on Seekonk Public Schools' technology (except those specifically excluded by law, such as a student record) is subject to the Massachusetts Public Records law. No user should expect that electronic mail messages (even those marked "Personal") are private or confidential. Copies of all information created, sent or retrieved may be stored on the network's back up files. This information may be disclosed to law enforcement or other third parties without prior notice to or consent of the user, sender or receiver.

Deleting an email message does not actually 'delete' it. Any email sent through the Seekonk Public Schools' technology may be kept separate from the user's computer. Like all other correspondence dealing with official district business, e-mail and other electronically stored information should be retained in an electronic format as required by the Massachusetts Public Records Law, to the extent not a student record. Please consult the Public Records Division of the Office of the Secretary of the Commonwealth for details regarding how this law affects your particular file, document, e-mail message or record.

The Seekonk Public Schools reserves the right to examine data stored on users' personal machines on school grounds or at school functions when there is a reasonable suspicion of inappropriate activity to make sure that all users are in compliance with this Policy.

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 provides education, as part of our curriculum, to students as appropriate through all grade levels on online safety including cyberbullying 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 who 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.

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

Student Access to Computers and the Internet

Students and parents are required to read the Seekonk Technology Responsible Use and Internet Safety Policy and sign and return the Seekonk Public Schools Contract for Student Access to Technology Resources. Only those students whose parents have consented to technology use and Internet access will be allowed access to district technology and the Internet. Please note that in some cases students will be permitted to access technology at the discretion of the building administration. For example, access may be permitted for reasons such as: federal, state, and district assessments. Students are required to use technology devices and resources responsibly and for academic purposes as outlined in this policy.

Students providing support to the district may be granted 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.

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 that you represent
- Accessing inappropriate web sites, data, pictures, jokes, files, games, etc.
- Inappropriate chatting, email, 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
- Downloading any programs or downloading any files not relating to schoolwork
- Displaying or downloading any kind of sexually explicit offensive image or document. In addition, sexually offensive material may not be archived, stored, distributed, edited, or recorded using Seekonk Public Schools' network or computing resources
- Accessing personal online accounts by students
- Posting personal information about themselves or other people
- Participating in activities that the user would reasonably anticipate causing congestion on the network or to 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.

Electronic Communications

The school district provides staff and students with a Google Apps for Education (GAFE) account. This account includes access to Gmail, Drive, Docs, Sheets, Slides, Forms, Calendar, Classroom and a variety of other Google Apps. Google Apps allow users to share documents and files with district staff and other students. Assignments can be turned in electronically and project collaboration can be achieved easily.

Staff shall use district Gmail for all school-related email correspondence. All staff email is archived for seven (7) years and is considered property of the school district. Incidental or occasional use of email for personal reasons by district staff is permitted. Students will be assigned email accounts as needed for class work. All users are required to report inappropriate use of email and other Google Apps to an administrator.

The following email activity is prohibited:

- Discussing highly sensitive or confidential school department information
- Accessing, or attempting to access, another user's email account
- Using email to harass, discriminate, or make defamatory comments
- Using email to send inappropriate email 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 without the permission of an administrator
- Participating in any communication that facilitates the illegal sale or use of drugs or alcohol
- Transmitting information that the user would reasonably know could cause network congestion or harm to another user's data

Student Gmail (grades 6-12)

Email is a powerful tool for students to increase communication and collaboration. Students are only allowed to use their school Gmail for school-related purposes. Students are encouraged to check their email at least once per day. Teachers, coaches, or club leaders may send email to middle and high school students to communicate reminders, course content, or questions related to class work or extracurricular activities. Students may send email to district staff members with questions or comments regarding schoolwork. Students may email other students to collaborate on group projects and assist with school-related purposes.

Student Emails to Staff

Students are expected to use their Gmail accounts to email staff concerning school-related content and questions; however, there will be no requirement or expectation for staff to answer student email outside of their regular workday. Staff may choose to respond at their discretion. For example, an unanswered email to a teacher would not excuse a student from turning in assignments.

Student Email Guidelines

Email is to be used solely for school-related communication. The following email activities are prohibited:

- Sending harassing or offensive content via email, instant messages, or other modalities
- Intentionally sending email or instant messages containing a virus or other malicious content
- Sending or reading email or instant messages at inappropriate times, such as during class instruction
- Sending email or instant messages that violate the academic integrity of the educational process, such as: sharing test answers or promoting cheating in any manner
- Transmitting junk mail or chain letters
- Using the account of another person

Commercial Activities

Users may not use technology for commercial activities, product advertisement or political lobbying, including lobbying for office, when not directly related to an educational purpose of the Seekonk Public Schools.

Publishing

All publications of school, grade, department, group, or project pages that are displayed on any of the Seekonk Public Schools' technology shall be created and reviewed in conformance with this Policy and within any additional guidelines established by the Seekonk Public Schools.

The purpose of any site on the Seekonk Public Schools' website is to encourage and enhance teaching and learning and to provide users and electronic visitors with accurate and timely information about the Seekonk Public Schools.

- All web pages will be official publications of the Seekonk Public Schools.
- The Seekonk Public Schools will administer all website development and content.
- Seekonk Public Schools' webmasters will operate and maintain all websites. All users given web posting privileges on the Seekonk Public Schools' website are solely responsible for that posted content.
- All information posted on the website must be in an accessible format.
- Members of the school community are encouraged to have input into the website, but the Seekonk Public Schools oversees all content.
- Individual teachers will review their students' material before publication for quality and completeness. All work must follow copyright laws.
- Students' photographic images, MAY NOT be published on a Seekonk Public Schools' web page without written consent from the parent/ guardian.

    1. No home addresses, telephone numbers or e-mail addresses of students will be posted.

    2. No student shall be identified by his/her full name.

    3. Students must submit a signed permission form from their parent/guardian granting permission to post the student's work.
- Logos or trademarks used must have written permission from the person or organization that owns the logo or trademark.

Social Media

Uses of web-based 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 social media. In addition, district rights, such as access and logging, to network resources extend to social media. By signing the appropriate Student Contract, parents are agreeing to allow their child permission to access these resources.

Definition:
Social media is defined as any form of online publication or presence that allows interactive communication, including, but not limited to, social networks, blogs, Internet websites, Internet forums,

and Wikis. Examples of social media include, but are not limited to; Facebook, Twitter, YouTube, Instagram, Snapchat, and Flickr.

Social Media Use

Social media technology can serve as a powerful tool to enhance education, communication, and 21st century learning. These technology tools can provide educational and professional benefits, including preparing Seekonk students to succeed educationally and in future career endeavors.

The Seekonk School District is committed to ensuring that all stakeholders, including staff and students, who utilize social media technology for professional purposes described below, do so in a safe and responsible manner. The district strives to create professional social media online environments that mirror the academically, supportive environments of our schools.

In recognition of the public and pervasive nature of social media communications, as well as the fact that in this digital era, the lines between professional and personal endeavors are sometimes blurred, this policy addresses acceptable practices for use of personal social media by staff, volunteers, coaches, and others who interact with Seekonk students on behalf of the district.

Differences Between Professional and Personal Social Media Activity:

- Professional social media is a work-related social media activity that is school-based (e.g., a principal establishing a Facebook or Twitter page for his/her school or a teacher establishing a Facebook, Twitter, or blog page for his/her class.)

- Personal social media use is a non-work-related social media activity (e.g., an administrative employee or school-based employee establishing a Facebook page or a Twitter account for his/her own personal use).

Professional Social Media Use Guidelines

Maintaining Separate Professional and Personal Email Accounts
District employees who decide to engage in professional social media activities should maintain separate professional and personal email addresses. As such, district employees should not use their personal email addresses for professional social media activities, rather, employees should use a professional email address that is completely separate from any personal social media account they maintain.

Communication with District Students
District employees who communicate with students through professional social media sites should develop sites that are school-based and are designed to address reasonable instructional, educational, or extracurricular program matters.

Professional Social Media

Seekonk School District employees and students should treat professional social media spaces and communication as they would in an instructional setting and/or a professional workplace. In other words, if a particular type of behavior is inappropriate in a professional workplace or classroom, then that same behavior is also inappropriate on a professional social media site.

When establishing professional social media sites, supervisors and employees should consider the intended audience for the site and consider the level of privacy assigned to the site, specifically, whether the site should be a private network (for example, it is limited to a particular class or particular grade within a school) or a public network (for example, anyone within the school, a larger group within the community can participate or individuals outside of the district). It is recommended practice for professional social media sites to be private networks, unless there is a specific educational need for the site to be a public network.

District employees must obtain their administrator's approval in writing before setting up a professional social media presence. Administrators or their designees are responsible for maintaining a list of all professional social media accounts within their particular school or office.

Professional social media communication must be in compliance with existing policies and applicable laws, including, but not limited to, prohibitions on the disclosure of confidential information and prohibitions on the use of harassing, obscene, discriminatory, defamatory or threatening language.

There must be a signed media consent form on file for each child featured if student images are to be posted online.

District students who participate in professional social media sites may not be permitted to post or identify photographs or videos featuring other students without the approval of the student and the teacher or other employee responsible for the site.

It is not recommended that employees post photos of other employees on professional social media sites without prior permission of the photographed employee.

Monitoring of Professional Social Media Sites

Administration, or their designees, are responsible for monitoring and providing feedback regarding their employees' professional social media sites. The monitoring responsibilities include reviewing the professional social media sites on a regular basis. If supervisors discover questionable communications or behavior on professional social media sites, they are required to contact the appropriate authorities for assistance.

Administration, or their designees reserve the right to require removal of postings and/or disable a page, if a staff member's professional social media site does not adhere to the law or does not reasonably align with this policy.

Personal Social Media Use

Communication with District Students
In order to maintain a professional and appropriate relationship with students, district employees should not communicate (this refers to activity, including, but not limited to, "friending," "following," "commenting," and "posting" messages) with students who are currently enrolled in Seekonk Public Schools on personal social media sites or by personal cell phone or other electronic devices. District employees' communication with students via personal social media is subject to the following exceptions: communication with relatives or in case of an emergency situation requiring such communication. Staff members should not give out personal contact information with current students without the prior approval of the Seekonk Public Schools.

All electronic communication with students should be through the district's computer or telephone system, except emergency situations or where prior approval is given for sites exclusively used for homework, classroom notices, or off campus activities, etc. as previously noted in this policy.

Applicability

These Guidelines apply to all employees and students. The district will take steps to ensure that other stakeholders, including vendors, volunteers, consultants, and independent contractors are informed of these Guidelines.

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, such as having antivirus 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 Responsible Use and Internet Safety Policy immediately to your building administrator and/or the Technology Department. Noncompliance with the school district's Responsible Use and Internet Safety 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:

- Suspension or revocation of network privileges either temporarily or permanently
- Suspension or revocation of computer access privileges either temporarily or permanently
- Suspension (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

Violations of the Responsible Use and Internet Safety Policy that may constitute a criminal offense may be referred to law enforcement authorities.

The following forms support this policy:

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

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

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

Seekonk Public Schools School Based Social Media Registry Form