ACCESS AND USE OF TELECOMMUNICATIONS SYSTEMS POLICY

The purpose of this policy is to set in place the standards for the proper and allowed uses of the Town's telecommunications systems and equipment, including but not limited to its computers, telephones, handheld devices, electronic mail (e-mail), facsimile machines (faxes), emergency notification systems, radio communication systems and the internet.

The Town's telecommunications systems and equipment, including computer hardware and software are valuable assets, owned by the Town, that should only be used for Town business; however, brief and occasional personal use of the e-mail or the internet is acceptable as long as it is not excessive or inappropriate, occurs during personal time (lunch or breaks), and does not result in expense or harm to the Town or otherwise violate this policy. Use is defined as "excessive" if it interferes with normal job functions, responsiveness, or the ability to perform daily job activities. Electronic communication should not be used to solicit or sell products or services that are unrelated to the Town's business; political activity, fundraising activity or distract, intimidate, or harass coworkers or third parties; or disrupt the workplace. All electronic equipment and software are the property of the Town of Seekonk and the Town may monitor at any time; therefore, town employees should not expect any privacy on any telecommunications system or equipment. The Town has the right to inspect any and all files stored in private areas of the network or on individual computers or stage media in order to assure compliance with town policies and State and Federal laws. Notwithstanding the Town's right to retrieve and read any email messages, faxes or internet postings generated from or sent to a Town-issued address, employees shall not retrieve or read any messages that are not sent to them unless express permission is given by the intended recipient.

No Expectation of Privacy/Public Access:
The Massachusetts Public Records Law broadly defines the term "public record" to include all documentary materials or data, regardless of its physical form or characteristics, created or received by any official or employee of any governmental unit. As a result, all photographs, papers and electronic storage media including e-mail of which a governmental employee is the "custodian" constitute "public records." Therefore, use caution as emails, faxes, records of phone calls made and received, and internet sites visited can be considered public information and can be reviewed not only by the Town, but also any third party who has the legal right to request the information in accordance with Mass Law. All emails sent and received as principal addressee at a Town-issued address, or any address when in an official capacity, as well as faxes and internet postings should be considered a public record subject to legal discovery and record retention policies.

Use of the Town's computers, networks, and internet access is a privilege granted by management and may be revoked at any time for inappropriate conduct carried out on such systems. The use of a password is to control access to the equipment and is not intended to create a right or expectation of privacy. All employees are required to register any computer passwords with the Director of Municipal Finance. All messages sent or received by email or the internet are stored automatically on the Town's computer system and deleting such messages does not guarantee that they cannot be retrieved.

Examples of Inappropriate Use:

- Using computers for unlawful or malicious activities;
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages or to offend, harass, abuse or otherwise communicate offensive, unlawful, or inappropriate messages or messages;
- No user shall pirate software or download and transfer software for which the user does not have the proper licensing;
- All users are expected to undertake precautions to prevent infection of Town computers by computer viruses. Executable programs imported from other sites to Town computers may not be used unless they have been authorized by the Director of Municipal Finance, or his/her designee, and have been subjected to virus detection procedures approved by the Town Administrator, or his/her designee;
- Users shall not engage in activities that could cause congestion and disruption of networks and systems, including but not limited to consuming excessive system resources, e.g. mail bombing and flooding;
- For security purposes, employees should either log off or revert back to a password screen saver when leaving their computer for an extended period of time. When leaving for the day, employees should log off;
- Installation of computer software and hardware is only to be done by the Director of Municipal Finance or his/her designee;
- Many computer files contain sensitive and privacy-protected data. Release of this data, whether deliberate or accidental, to unauthorized persons or agencies, may result in disciplinary action, up to and including termination;
- Viewing or transmitting pornography from Town systems is strictly forbidden;
- Employees may not take any computer equipment or software out of the workplace without written permission from the Town Administrator. Copying Town-owned software for personal use is a violation of software license agreements and is therefore forbidden;
- Making unauthorized copies of Town Files or other Town Data;
- Misrepresenting oneself or the Town;
- Destroying, deleting, erasing or concealing Town files or other town data, or otherwise making such files or data inaccessible to the Town or to other authorized users of the Town Systems;
- Engaging in private or personal business activities, including excessive use of instant messaging and chat rooms and using recreational games;

Any employee who violates this policy or uses the Town's telecommunications systems for improper purposes shall be subject to discipline, up to and including discharge.

Confidentiality of Email

As noted above, electronic mail is subject at all times to monitoring and the release of specific information is subject to applicable state and federal laws and Town rules, policies, and procedures on confidentiality. Existing rules, policies, and procedures governing the sharing of confidential information also apply the sharing of information via commercial software. Since there is the possibility that any message could be shared with or without

your permission or knowledge, the best rule to follow in the use of electronic mail for non-work-related information is to decide if you would post the information on the office bulletin board with your signature.

It is a violation of Town policy for any employee, including system administrators and supervisors, to access electronic mail and computer systems files to satisfy curiosity and to have engaged in such activities will be subject to the disciplinary action.

Electronic Mail tampering

No employees shall send email under another employee's name nor shall any employee change any portion of a previously sent email message without prior authorization.

Policy Statement

The internet is to be used to further the Town's mission, to provide effective service of the highest quality to the Town's residents and staff, and to support other direct job-related purposes. Employees are individually liable for any and all damages incurred as a result of violating the Town's security policy, copyright and licensing agreements. All Town policies and procedures apply to employees' conduct on the internet, especially, but not exclusively, relating to: intellectual property, confidentiality, town information dissemination, standards of conduct, misuse of company resources, anti-harassment, and information and data security.

This policy was approved and adopted by the Board of Selectmen on August 29, 2012, and amended by the Board of Selectmen on April 18, 2018.