TECHNOLOGY POLICY

I. Purposes. This policy provides the rules and regulations pertaining to the use, security, and maintenance of the Town's computer system. This policy also ensures that the Town's computer system is used solely to support Town functions and to inform employees of their responsibilities in using the computer system.

II. Definitions. The following definitions shall apply to this policy:

Computer system – The Town's computers, networks, servers, internet service, email service, data storage, printers, scanners, and other similar technological equipment.

Network & Systems Technician – The Town's appointed Network & Systems Technician.

III. Authority. The Network & Systems Technician shall have authority over the maintenance, management, and protection of the computer system, and to establish standards and protocols for these purposes. The Network & Systems Technician shall have enforcement authority for this policy. Any questions regarding this policy shall be directed to the Network & Systems Technician.

IV. Acceptable Use. Employee access to the computer system is solely for the performance of Town employment duties. Absent the prior approval of the Network & Systems Technician, any use that is inconsistent with this acceptable use is prohibited.

V. Prohibited Uses. Absent the prior approval of the Network & Systems Technician, the following uses are prohibited:

A. Software. Software, including updates, shall not be downloaded or installed on the computer system. Any downloaded or installed software shall be licensed to the Town. No unauthorized software shall be added to the computer system, including screensavers or games.

B. Personal devices. Personal devices shall not be attached to or access the computer system.

C. Remote Access. Remote access to the computer system from home or non-Town owned devices is prohibited.

D. Protection software. The disabling or removing of virus and malware protection software is prohibited.

E. Other Prohibited Uses. Any use that is inconsistent with this policy or other policies, rules or regulations of the Town or any determination by the Network & Systems Technician is prohibited, including but not limited to:

1. Any use that is illegal.

2. Any use that is obscene, sexually explicit or sexually suggestive.

3. Any use that represents personal views as the views of the Town.

4. Malicious use or deliberate disruption of the computer system.

5. Misuse or deliberate damage to the computer system.

6. Any use unrelated to the employee's Town employment.

7. Any use that is threatening or harassing to a person or entity.

8. Any use for religious, political, or personal gain purposes.

9. Any private advertising, marketing or soliciting products or services.

VI. Security.

A. Data protection. The computer system shall have licensed virus and malware protection software installed or approved by the Network & Systems Technician. The disabling or removal of Town-installed protection software is prohibited. Virus protection shall be active and licensed on all town computers.

B. Passwords. Employees are responsible for safeguarding their passwords for access to the computer system. ***Individual passwords shall not be printed, stored online, or given to others.*** Employees are responsible for all transactions made using their passwords. Employees shall not access the computer system with another employee's password.

C. Virus and Malware Software. The Town uses a variety of means to protect the computer system including security settings in software applications, virus scanning software, and firewalls. Employees shall not alter, or attempt to alter, any security setting. Employees shall not disable virus protection or attempt to bypass firewall protections without the prior approval of the Network & Services Technician.

D. **Privacy.** The Town retains control, custody and supervision of the computer system. Employees waive and have no expectation of privacy in their use of the computer system. The Town reserves the right to at any time to inspect and/or monitor computer system files, logs and other activity including emails stored on any part of the computer system. Monitoring may also include surveillance programs designed for that purpose.

E. **Backup and Recovery.** The Network & Services Technician shall be responsible for developing and maintaining the backup and recovery for the computer system. Any request for access to backup or recovery shall be made to the Network & Services Technician.

F. **Disposal.** No part of the computer system shall be disposed of, sold, donated or transferred to another person or entity without the prior approval of the Network & Services Technician. Any part of the computer system with data storage shall be recycled through an NYS EERA Covered Electronic Equipment recycling company which shall be an authorized NYS Data Destruction contractor. The Network & Services Technician shall maintain certificates of recycling and NAID certificate of data destruction.

G. **Copyrights.** Employees shall comply with all laws pertaining to the reproduction, use or distribution of copyrighted or otherwise protected materials. Employees shall comply with all licensing requirements. Employees shall not make copies of software other than those copies authorized in the software license. Employees shall respect the copyrighted protection of materials found on the internet.

VII. Internet Use.

A. **Access.** Employee access to the internet by means of the computer system shall be arranged by the Network & Services Technician who has the authority to restrict or prohibit internet use to any employee for violation of the requirements of this policy.

B. **Allowed Use.** Employee use of the internet by means of the computer system shall be solely in connection with the employee's Town duties and responsibilities.

C. **Prohibited Use.** In addition to the prohibited uses stated in Section V, employees shall exercise care in selecting websites to visit on the internet.

Viruses may be transmitted simply by viewing a site that contains computer code written to transmit viruses to others. Employees shall not use the internet for streaming media applications.

D. Privacy. An employee's internet use is neither personal nor private. The Town reserves the right to log network use and monitor file server capacity by employees. The Town and the Network & Systems Technician may assess an employee's use of internet services:

1. to determine that use of internet services and the computer system is consistent with this policy and the Town's other polices, rules and regulations;

2. to diagnose and resolve technical problems involving the computer system; or

3. to investigate possible misuse of internet services when a reasonable suspicion of abuse exists or in conjunction with an appropriate investigation.

VIII. Emails. The following requirements are use of the Town's email system.

A. Access. Employee access to the Town's email system shall be arranged only by the Network & Services Technician who has the authority to restrict or prohibit email service to any employee for violation of the requirements of this policy.

B. Allowed Use. Employee use of emails shall be solely for Town business. Employees may use email to communicate outside of the Town when such communications are related to Town activities and are within their job responsibilities.

C. Prohibited Use. In addition to the prohibited uses stated in Section V, employees shall not use email for illegal, disruptive, unethical or unprofessional activities or for personal gain, or for any purpose that would jeopardize the legitimate interests of the Town.

D. Privacy. The use of email services is neither personal nor private. Employees are prohibited from accessing another employee's email without his or her permission. The Town and the Network & Systems Technician may assess an employee's use of email services:

1. to determine that use of email services and the computer system is consistent with this policy and the Town's other polices, rules and regulations;

2. to diagnose and resolve technical problems involving the computer system; or

3. to investigate possible misuse of email when a reasonable suspicion of abuse exists or in conjunction with an appropriate investigation.

E. NYS Freedom of Information Law ("FOIL") and legal actions. Any email sent or received in conjunction with Town business may:

1. be releasable to the public under FOIL; and

2. require special measures to comply with any protections of personal privacy under law; and

3. emails, including personal communications, may be subject to discovery proceedings in legal proceedings.

F. Security. Employees shall take all reasonable precautions, including safeguarding and changing passwords, to prevent the use of the email system by unauthorized persons.

G. Management and retention of emails.

1. The retention and disposition of emails, including attachments, are governed by the NYS Local Government Records Law (Arts & Cultural Affairs Law Article 57-A) and the Record Retention and Disposition Schedule MU-1 (The University of the State of New York, The State Education Department, New York State Archives, 2003, as may be amended).

2. Employees should remove all emails from the email system in a timely fashion. If an employee needs to retain information in an email for an extended period of time, the employee should transfer it from the email system to an appropriate electronic or other filing system.

3. The Town is authorized to remove any information retained in an email system that is more than 60 days old. Employees shall be

notified prior to this action to give them the opportunity to save any message they need to retain.