Town of Montreat
Technology Use Policy

ADOPTED: March 12, 2015

1. **Scope and Ownership.** This policy applies to all Town of Montreat technology systems owned, leased, or otherwise operated by Town of Montreat. Town Technology Systems includes hardware, software, voice/data networks, user accounts, and associated processes/services. The scope of the policy covers use of Town Technology Systems by all employees, elected or appointed Board and Committee members, and other users who have access to Town Technology Systems (employed by the Town or not).

   Systems containing Town of Montreat data which are hosted by third parties outside of the Town of Montreat network, and the personnel with access to those systems are also subject to this policy. All technology resources defined in this section, along with all information transmitted by, received from, and stored upon said systems are considered to be possessed by, and/or the property of Town of Montreat. Additionally, all documents composed and messages and attachments composed, sent, received or stored on Town Technology Systems are Town of Montreat property.

2. **Policy Violation.** When a policy violation occurs, aside from disciplinary actions specified under Town policy, system access may be revoked in whole or in part if deemed to be in the interest of Town Technology System security.

3. **Personal Use.** Town Technology Systems are intended for business use. Any incidental or occasional personal use must adhere to the following:

   - must not violate this Policy or any applicable laws or regulations;
   - must not violate contractual agreements or intellectual property rights ;
   - must not violate the Town of Montreat Personnel Policy;
   - must not incur security risks to the Town;
   - must not incur any additional cost to the Town;
   - must not interfere with work duties, work performance or work productivity;
   - must not be used for personal gain;
   - must not be used for solicitation

4. **Monitoring and Privacy.** The Town of Montreat has the right to monitor, audit, and/or inspect any and all aspects of the Town Technology Systems at any time, without advance notice to any users, and without the permission of any user. Failure to monitor in any specific situation does not constitute a waiver of the Town's right to monitor. Users within the scope of this policy are advised that they have no privacy rights and no user of Town Technology Systems has any expectation of privacy in any message, file, image, or data sent, retrieved, or received when using Town Technology Systems.

A. Monitoring, Auditing, and Inspection Activities. Upon authorization by the Town Administrator or his/her designee, any Town Technology System may be monitored or inspected without notice to users.

For security, network, and computer systems maintenance purposes, authorized individuals may monitor equipment, systems, data and network traffic at any time.

For remote assistance help desk purposes, authorized individuals may connect through remote access software to equipment, systems, data and network traffic at any time.

B. Privacy Expectations. The Town does not guarantee the confidentiality of user information stored on any network, computer, or communications device belonging to Town of Montreat. Town of Montreat's users should be aware that the data they create on Town technology or communications systems remains the property of Town of Montreat and is not private (unless the data is protected by privacy or confidentiality laws). Information that is stored on or transmitted to or from Town Technology Systems may be subject to disclosure pursuant to the North Carolina Public Records Law.

5. Security. Town Technology System security must be maintained at all times. Users must take all reasonable precautions, including but not limited to: safeguarding passwords, maintaining reasonable physical security around the Town of Montreat equipment, and locking or logging off unattended workstations.

A user who is actively logged on to a Town of Montreat system is responsible for any activity that occurs whether or not the user is present.

A. Administrative Privileges. For security reasons, administrator-level network, server, and PC access, is limited to designated Town staff members and authorized third-party vendors.

Administrator privileges will not be extended to users in order for software to operate. Software vendors are responsible for providing software that will operate without administrator privileges.

B. Passwords and User System Access. The Town Administrator, Town Clerk, their designee(s), and third-party technical support vendors are responsible for creation, assignment, and deletion of all user accounts for Town Technology Systems. The level of access to the network, servers, applications, and personal computers will be determined based upon the job tasks for the individual user as agreed upon with the department head. Users are responsible for protecting their passwords and access to assigned accounts (network, systems, applications, etc.) at all times.

C. Physical Security. Shared Town of Montreat systems (network, servers, systems, etc.) will be physically secured through the following procedures:

- Access to the server room, disaster recovery site, phone switches, and other key infrastructure is limited with access granted to authorized personnel only.
- Media, such as daily and monthly backups, will be stored in a secure area with access granted to authorized personnel only.
- Users are responsible for the physical security of assigned technology resources.
- To the degree possible, technology resources should be protected from theft and/or vandalism, fire and other natural environmental hazards.
- Laptops, cell phones, and other electronic devices in vehicles must be stored in a secure location or otherwise out of sight. They may never be left in a vehicle over night.
- Users should exercise precautions to make sure that their computer hardware is not exposed to dangers related to their specific use, such as accidental beverage spills, improper ventilation of air intakes, etc.

D. Application Security Standards. All software applications which manage sensitive or confidential data, whether acquired from a third party or developed internally must adhere to the following security requirements:

- Must support authentication of individual users;
- Must not store or transmit user credentials in a clear text or easily reversible form;
- Must support application scope restriction based on user levels;
- Must support user tracking for critical transaction activity.

E. Third Party Access to Town of Montreat Systems. No third party may be allowed access to Town of Montreat systems without prior authorization approval from the Town Administrator or his/her designee.

F. Reporting Violations. It is the responsibility of each technology user to remain diligent in the identification and reporting of technology policy violations. Staff should be aware of their environment and report any suspicious, abnormal or unnatural behavior or events to the Town Administrator or a supervisor.

6. **Prohibited Use.** The following is a list of examples of prohibited uses of Town Technology Systems. This is not intended to be a comprehensive and complete list. Other uses not listed here may be deemed as prohibited.

- Any use that violates federal, state, or local law or regulation is expressly prohibited.
- Knowingly or recklessly interfering with the normal operation of computers, peripherals, or networks is prohibited. This includes, but is not limited to, the installation, downloading or running of non-approved software applications, programs or executable files and accessing, downloading, printing or storing material or information in the following categories:

Adult/Sexually Explicit	Alcohol & Tobacco	Gambling	Intimate Apparel
Peer-to-Peer	Personals & Dating	Proxies & Translators	Ringtones/ Mobile
Spam URLs	Tasteless & Offensive	Hacking	Intolerance & Hate
Phishing & Fraud	Illegal Drugs	Online Gaming	Online Chat
Web Hosting	Web-Based Downloads		

- Connecting unauthorized equipment (Digital Cameras, Webcams, Microphones, Personal Printers, etc.) to the network for any purpose is prohibited without prior approval from the Town Administrator.
- Copying of any software from Town of Montreat computers is prohibited.
- Using the Town of Montreat's network to gain unauthorized access to any computer system is prohibited.
- The use of Town of Montreat Systems to access, transmit, store, display, or request obscene, pornographic, erotic, profane, racist, sexist, libelous, or other offensive or abusive material (including messages, images, video, or sound) is prohibited.
- The use of Town of Montreat Systems in such a way as to create an intimidating or hostile work environment is prohibited.
- Town of Montreat Systems may not be used to solicit for personal gain or for the advancement of a political or religious belief.

7. **Remote Access.** Remote access to Town of Montreat systems (access to Town of Montreat systems from external systems, e.g. via the Internet) consumes technology resources above and beyond those required for local access. Remote access shall be granted on a case-by-case basis based upon the unique needs of the user and available resources. Remote access users are subject to all policies herein.

8. **Hardware/Software Procurement, and Installation.** Procuring, receiving, maintaining, and installing hardware or software for or on Town of Montreat networks shall be done only by the Town Administrator, Town Clerk, their designee(s), or approved third-party vendors. Town of Montreat departments may procure, receive, install, and utilize computer equipment from the private sector on an individual basis. Such activities require prior confirmation from an authorized third-party technology support vendor to ensure that the equipment meets Town standards and will not interfere with current Town Technology Systems.

9. **Electronic Messaging.** Electronic messaging includes, but is not limited to email, instant messages, text messages, blog posts, forum posts, wiki posts, images and audio or video recordings. Electronic messages may be considered public record and as such are subject to public record retention rules. Electronic messaging may not be used in any way which violates Town policy.

10. **Town Internet Content.** Public Internet content includes but is not limited to the main Town of Montreat public web site and all content therein. Editing and publishing Town of Montreat public Internet content is the responsibility of the Town Administrator, Town Clerk or their designee(s). Each department is solely responsible for the accuracy of the content of their respective web site(s) and/or pages. Links to personal websites are not allowed. Information on events will be limited to those directly sponsored by or affiliated with the Town of Montreat.

11. **Policy Review.** This policy is subject to review and revision at any time pursuant to recommendations from the Town of Montreat Board of Commissioners or staff.