**TOWN OF AVON**

**POLICY MEMORANDUM**

SUBJECT: Acceptable Use Policy

NO: 11.2
DATE: September 6, 2022
BY: Town of Avon, Information Technology Committee

APPROVED: _____
Brandon Robertson
Town Manager

I. PURPOSE

The purpose of this policy memorandum is to establish uniform regulations to be followed by anyone with authorized access to Town technology assets through any technological equipment, whether owned or leased by the Town, or owned or leased by a third party. Specifically, this policy shall apply to regular and temporary employees, elected officials and third party personnel such as consultants or contractors.

Inappropriate use of technology assets can expose the Town to risks including malware attacks, data loss, compromise of network systems and services, and legal issues.

II. RESPONSIBILITY

It shall be the responsibility of the Town Manager to ensure the implementation of and adherence to this policy by all Users.

It shall be the responsibility of the Town's Information Technology Committee Chair to review and respond to user requests for access to or installation of Town technology assets and to ensure the IT Committee reviews this policy annually and recommends relevant edits and updates if warranted.

It shall be the responsibility of all Town department and division heads to communicate their users' requests for access to or installation of Town technology assets once determining the need is related to the scope of their work.

It shall be the responsibility of all users to read and understand this policy and to conduct their activities accordingly. All users shall sign the Acceptable Use Policy Acknowledgement Form (Appendix A) prior to being granted access to Town technology assets or equipment.

III. NETWORK ACCESS

Users should not expect privacy while utilizing Town technology assets or Town technology equipment. The Town reserves the right to monitor, log, or audit use of such assets or equipment at any time to ensure compliance with this policy.

All data or other materials created on, or through the use of, Town assets shall remain the property of the Town. The Town may access all information stored on any equipment belonging to the Town at any time.

Users shall not disable security measures, devices or software on any Town resource unless explicitly authorized to do so by the Town Manager.

Technology assets and equipment shall be used by employees for purposes of performing work within the scope of their employment and should not be used for other reasons or purposes. The Town does recognize that there are occasions that require limited use for personal reasons, but the Town reserves the right to audit or otherwise investigate whether a user is using the Town's technology assets or equipment for personal reasons beyond these limited occasions.

## IV. SENSITIVE INFORMATION

Employees may be privy to sensitive information (which may include private data, confidential information, or Personally Identifiable Information (PII)) in the course of their work. It shall be the responsibility of users interacting with such information to maintain and safeguard it and to only use it in accordance with this policy.

All Users are responsible for protecting sensitive information on Town technology assets and equipment. Users shall be familiar with all applicable Town policies and procedures related to sensitive information and are responsible for understanding the implications of a breach of the sensitive information for which they are responsible.

Users are responsible for notifying their immediate supervisor or the IT Committee Chair in the event they suspect an information system security compromise that could lead to the exposure of sensitive information, or a known or suspected data breach. Theft of the Town's technology assets or equipment shall be immediately reported to the Town Manager and the Avon Police Department.

Town staff shall not divulge information regarding Town data to an outside party unless such distribution is required for Town business or in response to a request that is properly submitted to the Town pursuant to the Freedom of Information Act (Conn. Gen. Stat. § 1-200 *et seq.*). If information about the Town has not been made public by the Town it should be treated as sensitive.

Users shall not share sensitive data via unencrypted/unsigned email or collect sensitive data with web forms that are not secured with Hypertext Transfer Protocol Secure (HTTPS) connection with a valid Secure Sockets Layer (SSL) certificate. Sensitive information shall be stored on a centrally managed Town Server or on a cloud service with whom the Town has a contractual relationship.

Users shall employ passwords that comply with Section V below, keep local applications updated and patched; encrypt sensitive files with Town-approved methods; and ensure that remote access connections, as approved by the IT Committee Chair, are made securely using HTTPS, Secure Shell Protocol (SSH), or Virtual Private Network (VPN).

Users that receive sensitive information in error shall inform the sender and properly delete/destroy the copied information.

## V. PASSWORD COMPLIANCE

All Users shall keep passwords secure and accounts should not be shared. Passwords shall adhere to the following requirements:

- Passwords shall be changed, at minimum, every 90 days;
- Passwords shall not be written down;
- Passwords shall not contain the User's legal name;
- Passwords shall be at least eight (8) characters and shall contain a combination of lowercase, uppercase, numbers and special character;

## VI. WORKSTATION COMPLIANCE

Workstations shall be secured when left unattended. Users may secure their workstations using a password-protected screensaver with the automatic activation feature set to fifteen (15) minutes or less; manually locking the computer using "Ctrl-Alt-Delete," or logging off.

Users shall not install any software on Town technology equipment. Installation of software shall be requested and performed through the Town's managed service provider or the IT Committee Chairperson. Users shall not circumvent security measures placed on Town technology assets or equipment in order to install unauthorized software.

## VII. WIRELESS ACCESS

Unless authorized by the IT Committee Chair, users shall only connect Town equipment to secured Town wireless access points. Personal devices, guest devices or third party devices should connect only to open, guest wireless networks.

## VIII. REMOTE ACCESS/VIRTUAL PRIVATE NETWORK (VPN)

Users may require remote access to the Town's network in order to perform work functions. Requests for remote access shall be submitted to the IT Committee Chair by the user's supervisor for approval. In general, users shall only connect Town devices to the VPN. Access to the VPN via a personal device must be approved in advance by the IT Committee Chair. Approved personal devices must have an appropriate personal firewall, antivirus protection and malware detection installed as determined by the IT Committee Chair in consultation with the Town's managed service provider.

## IX. BRING YOUR OWN MOBILE DEVICE

The Town permits employees to use their own personal devices, such as smartphones, tablets, and laptops ("personal devices") to connect to the Town's network. However, to protect the Town and its employees, any use of a personal device must conform to these requirements and each user is responsible for using their personal device in a sensible, productive, ethical, and lawful manner while connected to the Town's network.

Any personal device that connects to the Town's network must:

1. be running a current supported version of Windows or Mac operating system;
2. be up to date with security patches;
3. have up to date Anti-Virus Software installed and operating; and
4. have an active firewall.

When at work, Town employees' personal smartphones are allowed to connect to the Town's guest wireless network. When not at work, or when outside of Town Hall, Town employees are permitted to use personal devices to access Town matters through (a) the Town's email via Outlook Web Access; and (b) the Town's SSL-VPN Portal.

Town data is expressly prohibited from being transferred to any personal device, whether the personal device is used for personal matters or Town matters.

Support for personal devices is through opening a helpdesk ticket by emailing helpdesk@coopsys.com or calling the helpdesk. Support for personal devices is limited to the permitted uses described herein.

## X. PROHIBITED EMAIL/COMMUNICATIONS ACTIVITIES

Users shall use caution when opening email attachments from unknown senders. The following activities are strictly prohibited:

- Sending unsolicited emails, such as junk mail or email spam;
- Participation in any forum, distribution service or UseNet group that disseminates illegal, inappropriate or otherwise questionable material;
- Any form of harassment via email, telephone or paging;
- Viewing, printing or transferring materials in violation of the Town's Sexual Harassment Prevention Policy;
- Downloading or receiving messages and attachments from an untrusted source that may contain viruses and/or malicious programs;
- Forging email header information;
- Solicitation of messages for any other email address, other than that of the poster, with the intent to harass or collect replies; and
- Creating or forwarding chain letters, Ponzi schemes, or other pyramid schemes.

This list is not exhaustive, and the Town reserves the right to supplement this list with additional activities.

## XI. UNACCEPTABLE USE

The following activities exemplify unacceptable use of Town technology assets and equipment. This list is not exhaustive. If a user is uncertain of the acceptability of a particular activity, the user shall consult the IT Committee Chair prior to performing the activity.

- Introducing or downloading malicious programs onto Town technology assets, such as viruses, worms, Trojan Horses, email bombs, other malware, etc.
- Using Town technology assets to actively engage in the procurement or transmittal of material that is in violation of the Town's Sexual Harassment Prevention Policy.
- Making offers of products, items, or services originating from any Town account, unless such action is within the user's scope of work.
- Breaching or disrupting network communications, i.e. authorized access to Town data; unauthorized access to a server or account; excessive network traffic; network sniffing; ping floods; packet spoofing; denial of service; etc.

- Network monitoring, port scanning, or security/vulnerability scanning. This includes "testing" security tools on any Town technology asset.
- Circumventing user authentication or Town access controls.
- Adding music, software or video downloads from any source, unless such action is within the user's scope of work.
- Installing, tunneling, or circumventing software with the direct or indirect aim of avoiding security measures or restrictions.
- Providing information about, or lists of, Town users, customers, clients, or candidates to parties outside of the Town without prior authorization by the Town Manager or his designee.
- Violating the rights of any person or company protected by copyright, patent, or other intellectual property or similar laws or regulations, including, but not limited to, installation or distribution of pirated materials or software products that have not been licensed for use by the Town.
- Duplication of copyrighted material such as digitization and distribution of photographs, music or software for which the Town does not have an active license.
- Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws.

Users may be exempted from any of these restrictions should their scope of work require that they perform the restricted activity in question. However, under no circumstances is a Town employee authorized to engage in any unacceptable activity outside of their scope of work. Questions about whether a specific task or activity is within a user's scope of work should be referred to the user's supervisor prior to engaging in such task or activity.

## XII. SOCIAL MEDIA GUIDELINES

Town social media accounts may be used to communicate announcements about department or community news, emergency notifications, Town events and activities and other items of interest.

Departments or Divisions must have prior approval from the Town Manager, or their designee, to establish a social media account on behalf of the Town. Unless authorized as a Designated User of the site by a Department or Division head, Town employees are not permitted to post content to Town social media sites.

Designated Users must adhere to all applicable state, federal, and local laws, as well as all Town regulations and policies, and they must conduct themselves at all times as representatives of the Town. The Town Manager, or the employee's Department or Division head, may revoke an employee's Designated User status at any time, for any reason.

Town social media accounts should not be used to express personal opinions. Unless specifically authorized by the Town Manager, employees are not permitted to speak on behalf of the Town via a personal social media account.

Please refer to Appendix B, "Designated User Guidelines for Use of Town Social Media Sites" for further guidance on the use of Town social media accounts.

## XIII. DEFINITIONS

A *User* refers to anyone with authorized access to Town technology assets through any technological equipment, whether owned or leased by the Town, or owned or leased by a third party. This shall include regular and temporary employees, elected officials and third-party personnel such as consultants or contractors.

*Malware* refers to software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

*Town technology assets* refer to all computing, networking, and software applications that can be accessed by Users.

*Technology equipment* refers to computing hardware, such as PCs, laptops, and smartphones.

*Traffic* refers to the management of the number of users and data on a communications device or system.

*Designated User* refers to a User who has been granted the responsibility of maintaining one or more Town social media accounts.

*Sensitive Information* collectively refers to private data, personally identifiable information, and confidential data.

*Private Data* refers to any information that is contractually protected as confidential by law or by contract and any other information that is considered by the Town to be appropriate for private treatment.

*Personally Identifiable Information (PII)* refers to any information about an individual that can be used to distinguish or trace an individual's identify, such as name or place of birth; information that is linked to an individual, such as medical, educational, financial and employment information; and information that is protected by federal, state or local laws and regulation or industry standards.

*Confidential Data* is any information protected by federal, state or local laws and regulations or industry standards. This category is subject to the most restricted distribution and must be protected at all times in accordance with applicable regulations.

## APPENDIX A
## ACCEPTABLE USE POLICY
## ACKNOWLEDGEMENT FORM

I understand that this page must be signed and returned to my supervisor and/or the Director of Human Resources before I am permitted to access the Town's technology assets or equipment including Town of Avon networks, computer systems, programs and the internet.

By signing below, I acknowledge that I have received and read the Town's Acceptable Use Policy governing the appropriate and acceptable use of Town technology assets and equipment.

I certify that I understand this policy, its application and its implications.

I understand that I will be held accountable for my actions, and should I violate this policy I understand that I may be subject to loss of access to technology assets or equipment, or additional actions, up to and including termination and/or civil and criminal legal action, as appropriate.

| | |
|---|---|
| **Printed Name:** | |
| **Title:** | |
| **Signature:** | |
| **Date:** | |

## APPENDIX B
## DESIGNATED USER GUIDELINES FOR USE OF TOWN SOCIAL MEDIA SITES

1. **Telephone, Computer Systems and Electronic Devices Policy.** All designated users are responsible for understanding and following the Town of Avon's Acceptable Use Policy.

2. **First Amendment Protected Speech.** Although the Town of Avon can moderate the social media sites that accept comments from the public to restrict speech that is obscene, threatening, discriminatory, harassing, or off topic, employees cannot use the moderation function to restrict speech with which the Town merely disagrees (i.e. subject matter restrictions). Users have some First Amendment rights in posting content to public social media sites hosted by municipalities. Designated Users must respect those rights by posting all comments other than those excluded for specific legitimate reasons, as follows:

    a) Random or unintelligible comments;
    b) Profanity, obscene, offensive, violent, or pornographic content and/or language;
    c) Content that promotes, fosters, or perpetuates discrimination or harassment on the basis of any legally protected status, including race, color, age, religion, gender, marital status, national origin, disability or sexual orientation;
    d) Defamatory or personal attacks;
    e) Threats to any person or organization;
    f) Content in support of, or in opposition to, any political campaigns or ballot item;
    g) Solicitations of commerce;
    h) Content demonstrating participation in, or encouraging, any illegal activity;
    i) Content that may compromise the safety or security of the Town or the public;
    j) Content that violates a legal ownership interest of any other party; or
    k) Any other content deemed inappropriate by the Town.

3. **Copyright Law.** Designated users must abide by laws governing copyright and fair use of copyrighted material owned by others. Never reprint whole articles or publications without first receiving written permission from the publication owner. Never quote an excerpt of someone else's work without acknowledging the source, and, if possible, provide a link to the original.

4. **Conflict of Interest**. Designated Users are prohibited from using social media to engage in any activity that constitutes a conflict of interest for the Town or any of its employees, as defined by the Town's Personnel Rules.

5. **Protect Confidential Information.** Never post legally protected personal information that you have obtained from the Town (e.g., information that is not public record under the Freedom of Information Act, or whose dissemination is restricted under applicable Federal or State privacy laws or regulations). Ask permission to publish or report on conversations that occur within the Town. Never post information about policies or plans that have not been finalized by the Town, unless you have received explicit permission from the Town Manager, or their designee (generally the user Department Head) to post draft policies or plans on the department's social media sites for public comment.

6. **Consider Your Content.** As informal as social media sites are meant to be, if they are on a government domain or a government identity, they are official government communications. Social media sites will be sought out by mainstream media – so a great deal of thought needs to go into how you will use the social media in a way that benefits both the Town and the public. Designated Users should not comment about rumors, political disputes, or personnel issues, for example.

7. **Handling Negative Comments.** Because the purpose of many social media sites, particularly department blogs and wikis, is to get feedback from the public, you should expect that some of the feedback you receive will be negative. Some effective ways to respond to negative comments include: a) Providing accurate information in the spirit of being helpful; b) Respectfully disagreeing; and c) Acknowledging that it is possible to hold different points of view.

8. **Respect Your Audience and Your Coworkers.** Do not use ethnic slurs, personal insults, obscenity, or engage in any conduct that would not be acceptable in the workplace. Do not be afraid to be yourself, but do so respectfully. This includes not only the obvious (no ethnic slurs, personal insults, obscenity, threats of violence, etc.) but also proper consideration of privacy and of topics that may be considered objectionable or inflammatory— such as party politics and religion. Do not use a Town sponsored social media presence to communicate among fellow Town employees. Do not air your differences with your fellow Town employees on Town sponsored social media sites.

9. **Use the Social Media Site or Identity Only to Contribute to your Department's Mission.** What you publish will reflect on the Town. Social media sites and identities should be used in a way that contributes to the Town's mission by: a) Helping you and your co-workers perform their jobs better; b) Informing citizens about government services and how to access them; c) Making the operations of your department transparent and accessible to the public; d) Creating a forum for the receipt of candid comments from residents about how government can be improved; and e) Encouraging civic engagement.

10. **Mistakes.** Once something is posted, it should stay posted. Only spelling errors or grammar fixes should be made without making the change evident to users. If you choose to modify an earlier post, make it clear that you have done so—do not remove or delete the incorrect content; provide the correct information and apologize for the error. Ways to accomplish this include: a) Strike through the error and correct; or b) Create a new post with the correct information, and link to it from the post you need to correct or clarify. Either method is acceptable. In order for the social media identity or site to achieve transparency, the Town cannot change content that has already been published without making the changes clearly evident to users.

11. **Media Inquiries**. Town sponsored social media identities or sites may lead to increased inquiries from the media. If you are contacted directly by a reporter, you should refer media questions to your direct supervisor and the Town Manager.

12. **Records Retention.** Social media sites will contain communications sent to or received by Town officials and employees, and are therefore public records. Ensure that the Town or department retains a copy of the social media content in accordance with public records retention schedules. Review the third party social media service provider's terms of service for its record retention practices. Note that while third party social media providers will most likely save your content for some period of time, they generally will not save it indefinitely. To the extent their policies are inconsistent with public records retention schedules, the Town or department should retain copies

of social media posts such as by printing or otherwise storing periodic "snapshots" of the social media sites.

13. **Freedom of Information Act.** Be aware of the Freedom of Information Act as it pertains to access to public meetings and possible violations for improper deliberations outside of a posted meeting. A series of individual postings on a social media site cumulatively may convey the position of a quorum of a governmental body regarding a subject within its jurisdiction and may constitute improper deliberation among the members of a board or committee, absent proper public notice of the meeting before such deliberation occurs.