USE OF TECHNOLOGY (COMMUNICATION) POLICY

ISSUE DATE:	AUGUST 2022	REVISION DATE:	

I. PURPOSE

To better serve our citizens and give our employees the best tools to do their job, the Town of Palmer Lake will continue to adopt and make use of new means to communicate and exchange information. Employees and officials may have access to one or more forms of electronic media and services, including, but not limited to computers, email, telephones, cellular phones, voice mail, fax, wire services, online services, networks, internet.

The Town encourages use of these media to communicate efficiently and effectively. However, all employees and officials should remember that electronic media, and services provided, is the property of the Town of Palmer Lake and the purpose is to facilitate Town business. **Note: All communications made by employees and officials are representing the Town of Palmer Lake.**

This policy cannot lay down rules to cover every possible situation. The purpose of this policy is to express general guidelines governing the use of electronic media and services.

II. POLICY

The following is procedure to this policy.

1. Access and Authority

a. Each supervisor shall determine which employees in their department shall have access to the various media and services, based on business practices and necessity and which shall have authority to communicate on behalf of the Town.

b. The provisions of this policy shall apply to the use of Town owned/provided equipment and/or services from home or other locations off Town premises. Town owned equipment (i.e., laptop, phone) may be removed from Town premises solely for Town work related purposes pursuant to prior authorization from the supervisor.

2. Prohibited Communications

a. Electronic media cannot be used for knowingly transmitting, retrieving or storing any communication that is:

i. Personal business on Town time (i.e., sports pools, games, shopping, correspondence or other non-business-related items/documents), except as otherwise allowed under #3 below;
ii. Discriminatory or harassing;
iii. Derogatory to any individual or group;
iv. Obscene, defamatory or threatening; or
v. For any purpose that is illegal or contrary to the Town's policy or business interests.

b. For the protection, integrity and security of the Town's system, electronic media shall not be used to download or transfer software, unless authorized by the supervisor.

3. Personal Use

a. Except as otherwise provided, electronic media and services are provided by the Town for employee business use during Town time. Limited, occasional, or incidental use of electronic media (sending or receiving) for **personal non-business** purposes is permitted as set forth below:

i. limited to breaks, lunch or immediately before/after work;
ii. must not interfere with the productivity of the employee or his or her co-workers;
iii. does not involve any prohibited activity;
iv. does not consume system resources or storage capacity on an ongoing basis;
v. does not involve large file transfers or otherwise deplete system resources available for business purposes.

b. Town telephones and cellular phones are to be used for Town business; however, brief, limited personal use is permitted during the workday.

c. Employees should not have any expectation of privacy with respect to personal use of the Town's electronic media or services.

Note: Use of Personal Devices - Do not connect personal devices to Town "Internal" networks.

4. Access to Employee Communications

a. Electronic information created and/or communicated by an employee using email, word processing, utility programs, spreadsheets, voice mail, telephones, Internet and bulletin board systems, desktop faxes, and similar electronic media is **public information** and may be accessed and monitored by the Town. The Town respects its employees' desire to work without surveillance. However, the Town reserves and intends to exercise the right, at its discretion, to review, monitor, intercept, access and disclose all messages created, received or sent over the electronic communication systems for any purpose including, but not limited to: cost analysis; resource allocation; optimum technical management of information resources; and detecting use which is in violation of Town policies or may constitute illegal activity. Disclosure will not be made except when necessary to enforce the policy, as permitted or required under the law, or for business purposes.

b. Any such monitoring, intercepting and accessing shall observe any and all confidentiality regulations under federal and state laws.

5. Security

A security policy exists to reduce the Town's exposure to cyber risks. The top three risks include unpatched software, social engineering, and poor passwords. The software risk is addressed by Administrative Privilege Policy and Network/Device monitoring. The social engineering risk is addressed by the Downloads Policy and by building "human firewalls" through training and phishing campaigns. The poor password risk is addressed by the Password Policy.

a. Browser Download Settings. All Town domain user accounts have permissions to download files. All Town browsers shall be set to "**Ask where to save each file before downloading."** For an intentional download, this helps the user know where the file has been saved. For an unintentional download, this alerts the user to a download attempt which can then be cancelled.

b. Passwords. Strong passwords will result in better security by incorporating lessons learned from past public data breaches. Where this policy conflicts with a compliance requirement (e.g., CJIS), the compliance requirement shall prevail. Periodic password resets are not required.

✓ MANDATORY:
- Each password shall be unique. Do not use a password that is the same or very similar to one used on any other computers or websites at work or home.
- Passwords shall be complex, that is, contain at least one each uppercase letter, lowercase letter, number, and special character.
- Passwords shall be at least 12 characters long.
- Keep passwords secret. Do not share them or leave them written down in your workspace.
- Use Multi-Factor Authentication (MFA) wherever possible.

✓ RECOMMENDED:
- Each "password" should really be an uncommon "passphrase." Do not use a single word (e.g., password) or a commonly used phrase (e.g., iloveyou).
- Consider using spaces and standard punctuation to increase length and complexity.
- Make passwords hard to guess even by those who know a lot about you.
- Use a password manager to encourage stronger passwords (add randomness and increase length) and make password management easier.

6. Appropriate Use

a. Employees and officials must respect the confidentiality of other individuals' electronic communications. Employees are prohibited from engaging in, or attempting to engage in:

i. Monitoring or intercepting the files or electronic communications of other employees or third parties;
ii. Hacking or obtaining access to systems or accounts they are not authorized to use;
iii. Using other people's logins or passwords; and
iv. Breaching, testing, or monitoring computer or network security measures.

b. No email or other electronic communications can be sent that attempt to hide the identity of the sender or represent the sender as someone else.

c. Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.

d. Anyone obtaining electronic access to other organizations', business', companies', municipalities', or individuals' materials must respect all copyrights and cannot copy, retrieve, modify, or forward copyrighted materials except as permitted by the copyright owner.

Employees must understand that the unauthorized use or independent installation of non-standard software or data may cause computers and networks to function erratically, improperly,

or cause data loss. Employees are not allowed to download any applications or software on any Town device. All updates on Town devices will be conducted through town staff and approved by the Town Administrator or designee.

Most of the Town's computing facilities automatically check for viruses before files and data which are transferred into the system from external sources are run or otherwise accessed. On computers where virus scanning takes place automatically, the virus scanning software must not be disabled, modified, uninstalled, or otherwise inactivated. If you are uncertain as to whether the workstation you are using is capable of detecting viruses automatically, or you are unsure whether the data has been adequately checked for viruses, you should contact designated Town staff.

Anyone receiving an electronic communication in error shall notify the sender immediately. The communication may be privileged, confidential and/or exempt from disclosure under applicable law. Such privilege and confidentiality shall be respected.

Note: Use of Town Devices - Do not connect town devices to public WiFi (for example, do not connect your town laptop to a coffee shop WiFi).

Note: Use of Web Portals - Do not login town or personal devices to town-related web portals on unknown public networks (e.g., coffee shop WiFi).

6. **Encryption**
   Employees who use encryption on files stored on a Town computer must provide their supervisor with a sealed hard copy record (to be retained in a secure location) of all the passwords and/or encryption keys necessary to access the files. Personal identifiable information requiring encryption includes the following items: address, date of birth, social security number, medical information, financial account information, driver's license, full face photos and other comparable images.

7. **Participation in online forums**
   a. Employees should remember that any message or information sent on Town-provided facilities to one or more individuals via an electronic network (for example: Internet mailing lists, bulletin boards, and online services) are **statements identifiable and attributable to the Town**.

   b. The Town recognizes that participation in some forums might be important to the performance of an employee's job. For instance, an employee might find the answer to a technical problem by consulting members of a newsgroup devoted to the technical area.

   c. Employees are encouraged to include the following disclaimer in their postings to public forums: *"The views, opinions, and judgments expressed in this message are solely those of the author. The message contents have not been reviewed or approved by the Town of Palmer Lake."*

   d. Employees should note that even with a disclaimer, a connection with the Town exists and a statement could be imputed legally to the Town. Therefore, employees should not rely on disclaimers as a way of insulating the Town from the comments and opinions they contribute to forums. Instead, employees must limit their discussion to matters of fact and avoid expressing

opinions while using the Town's systems or Town provided account. Communications must not reveal confidential information and must not otherwise violate this or other Town policies.

8. **Policy Violations**
   Employees who abuse the privilege of Town-facilitated access to electronic media or services risk having the privilege removed for themselves and possibly other employees, are subject to discipline, up to and including termination and may be subject to civil liability and criminal prosecution.

9. **Incident Response**
   In the case of suspected malware or cyberattack, follow these steps:

   a. Contact the Town IT consultant immediately
   b. Pull the plug – remove the affective device(s) from the network quickly by unplugging the cable, disconnect from WiFi or disconnect the power completely
   c. Change passwords as soon as possible – change all passwords on the affected device

Electronic communications may reside on the system in different recoverable forms (system backup, sent mail folders, spool queues, etc.). Employees and officials should not assume that deleting an electronic communication removes all incidents of its existence. If there is a review of the information or an investigation, litigation, or other proceeding that requires or makes desirable the review or production of Town records, it is likely that electronic communications will be requested and potentially disclosed. Moreover, employees should not delete any communications that are public record under C.R.S. Title 24 Public Records law.