CITY OF DENTON

POLICY/ADMINISTRATIVE PROCEDURE/ADMINISTRATIVE DIRECTIVE

SECTION:	GENERAL POLICIES/PROCEDURES/DIRECTIVES	REFERENCE NUMBER: 506.01
SUBJECT:	TECHNOLOGY SERVICES (TS)	INITIAL EFFECTIVE DATE: 10/01/2017
TITLE:	ACCEPTABLE USE OF TECHNOLOGY	LAST REVISION DATE: 03/04/2020

ADMINISTRATIVE DIRECTIVE

The purpose of this directive is to outline the acceptable use of computer equipment, technology systems, and communication devices at the City of Denton (City). These rules are in place to protect the employee and the City. Inappropriate use exposes the City to risks including virus attacks, compromise of network systems and services, and legal issues.

This directive applies to employees, contractors, vendors, and other authorized individuals who utilize any information technology, electronic, or other communication device owned and provided by the City, or who are granted access to any Local Area Network and/or Wide Area Network or other service maintained and provided by the City. This does not include computers that are designated for public use.

I. GENERAL USE AND OWNERSHIP

A. City resources are for City business: City-owned technology resources shall serve the business needs of the City of Denton.

B. Confidentiality: City-held information on the constituents, customers or employees of the City may not be disclosed without a clear business need or public disclosure request under applicable laws.

C. Sensitive Information: All employees are responsible for protecting Sensitive Information from unauthorized disclosure or release. Sensitive Information is defined as any combination of the following information:

- Social Security Number
- Personal identification numbers which may be used other than Social Security Number
- Information protected by the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Credit card account numbers
- Bank account numbers
- Lists of computer systems ID's and/or passwords

POLICY/ADMINISTRATIVE PROCEDURE/ADMINISTRATIVE DIRECTIVE (Continued)

TITLE: *ACCEPTABLE USE*	*REFERENCE NUMBER:* *506.01*

- Attorney/Client privilege information
- Any other information considered confidential

D. Devices and Media requiring Encryption: Encryption is required for all laptops, workstations, and portable drives that may be used to store or access City Sensitive Information. Departments who have a laptop, workstation, or portable drive that requires encryption should contact the Technology Services helpdesk at phone extension 8300.

E. Printer Use: The purchase or lease of copiers, printers, faxes, and scanners will be handled by request through the Technology Services department. No individual or department is authorized to purchase or lease these devices. Requests for additional or replacement equipment should also be made through Technology Services. Personal printers purchased by individuals with their own personal money are not allowed on the City of Denton network. If an employee is found to have violated this policy the device identification information will be recorded, and the violation will be reported to their department head. If further action is needed the device will be disconnected and the department head will consult with the Human Resources Director or designee on further action.

Printer request Procedure. Technology Services should be contacted and provided with an initial printer request. Technology Services will schedule an interview with the requestor and will conduct an assessment. The assessment will include the following;

- Location of current power, network, and analog service
- Number of users in the immediate area
- Applications, print job types
- Special Needs
- Sensitive Information
- Disability
- Current monthly usage (total output volume from printing, copying, and fax)

If a device is approved, Technology Services will coordinate the install of any network, power or analog services, if needed. When the device arrives, Technology services will contact the requesting department to schedule installation. After installation, Technology Services or the contracted print services vendor will conduct an onsite training session to ensure the device works correctly in the intended environment as well as to educate users on the features and capabilities of the device.

POLICY/ADMINISTRATIVE PROCEDURE/ADMINISTRATIVE DIRECTIVE (Continued)

TITLE: *ACCEPTABLE USE*	*REFERENCE NUMBER:* *506.01*

Printer Supplies. The following supplies for the normal operation of printers will be ordered and deployed by the Technology Services printer management contract. Technology Services has contracted out with a contracted print service for these services. These supplies include:

- All toner and ink cartridges
- Maintenance kits

The following supplies are not ordered by Technology Services but can be ordered through the City's approved vendor for supplies;

- Paper

Printer Support: All printers located within the department will be supported and maintained by the contracted print service staff unless the device is labeled otherwise. If the device is not supported by the contracted vendor, it will be Technology Services' responsibility. Although the devices supported by the contracted vendor are monitored for toner replacement, it will be the department's responsibility to contact the Technology Services Help Desk at x83000 when toner needs to be replaced.

When requesting support or service for a device in your department or division please follow these steps:

- Call the IT Help Desk or submit the request through x8300 or emailing servicerequest@cityofdenton.com
- Indicate the building and room number
- Indicate whether the device is supported by the contracted vendor or not. If the device is supported by the vendor, please report the service ID number located on the device
- Provide a brief description of the problem
- Provide your contact information

Before an actual service ticket is assigned to the contracted print service. Technology Services will make every effort to resolve the issue immediately. If the issue is not resolved immediately the TS Technician will initiate additional steps with the contracted vendor or other means to provide a solution.

F. Electronic Data Transfers: Any transfer of unencrypted City Sensitive Information must take place via an encrypted channel. Email messages containing encrypted data may never include the password in the same message as the encrypted data. Individuals who are unsure if they are correctly encrypting electronic data transfers should contact the Technology Services helpdesk at phone extension 8300.

POLICY/ADMINISTRATIVE PROCEDURE/ADMINISTRATIVE DIRECTIVE (Continued)

TITLE: *ACCEPTABLE USE*	*REFERENCE NUMBER:* *506.01*

G. Limited Personal Use: City-owned technology resources may be used for personal purposes on a limited basis, providing the following requirements are met:

1. No marginal cost to the City;
2. No interference with work responsibilities;
3. No disruption to the workplace;
4. No adverse impact to network or server performance; and
5. No personal gain.

H. Limited use of external e-mail services: The limited use of an external e-mail service is allowed, providing that the service applies anti-malware controls in a manner equivalent that is provided by the City.

I. Copyrighted Material: City computers must not be used to store copyrighted material that was not purchased by the City. Examples include but are not limited to music, audio files, video files, and digital books or magazines stored for personal use.

J. Use Standard Resources Only: Digital equipment and all applications must be authorized, purchased, and installed by the appropriate personnel. Only software, hardware, and communication protocols approved by Technology Services will be installed.

K. Additional Cost to the City: Resources that incur a cost to the City, whether accessed via the Internet, mobile, e-mail or other applications, must not be accessed or downloaded without prior approval. It is the supervisor's responsibility to assure the business need, applicability, and safety of any new resource. Proper procurement procedures must also be followed.

L. No Expectation of Privacy: Nothing in this directive confers an individual right or should be construed to provide an expectation of privacy. Employees must not expect privacy in the use of City communications and digital equipment.

M. Conflicts: If any component of this directive conflicts with any applicable laws or meet and confer agreement, the applicable law or meet and confer agreement shall control. The remaining non-conflicting features of this directive shall remain in effect.

II. UNACCEPTABLE USE

Under no circumstances is an employee of the City authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing the City's resources.

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities. The following lists are by

POLICY/ADMINISTRATIVE PROCEDURE/ADMINISTRATIVE DIRECTIVE (Continued)

TITLE: *ACCEPTABLE USE*	*REFERENCE NUMBER:* *506.01*

no means exhaustive, but an attempt to provide a framework for activities, which fall into the category of unacceptable use:

A. System and Network Activities

1. Unless specifically authorized, the use of personally owned technology for conducting City business, where official City records are created but not maintained by the City;
2. Making unauthorized general message distributions to all users (All Employees Distribution Group);
3. Installing any software not approved by Technology Services;
4. Sharing or storing unlicensed software or multimedia files;
5. Attempting to elevate user privileges or obtain unauthorized resources (hacking);
6. Intentional broadcasting e-mail to large numbers of recipients unless the list members are hidden through the use of the BCC field;
7. Introduction of malicious programs into the network or servers (e.g., viruses, worms, Trojan horses, email bombs, etc.):
8. Effecting security breaches or disruptions of network communications. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access unless these duties are within the scope of their duties; and
9. Circumventing user authentication or security of any hosts, network or user accounts.

B. Internet

1. Conducting a private business;
2. Political campaigning;
3. Accessing sites which promote exclusivity, hatred, or positions which are contrary to the City's policy of embracing cultural diversity;
4. Accessing inappropriate sites including adult content, online gambling, and dating services;
5. Accessing sites that promote illegal activity, copyright violation, or activity that violates the City's ethical standards;
6. Using the Internet to obtain or disseminate language or material which would normally be prohibited in the workplace;
7. Broadcasting e-mail to large numbers of recipients unless the list members are hidden through the use of the BCC field; and
8. Using a City e-mail address when posting to public forums e.g. blogs, wikis, and discussion lists for personal use.

POLICY/ADMINISTRATIVE PROCEDURE/ADMINISTRATIVE DIRECTIVE (Continued)

TITLE: *ACCEPTABLE USE*	*REFERENCE NUMBER:* *506.01*

C. Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam). Spam is an unsolicited email, normally with an advertising content sent out as a mass mailing. It typically has advertising content: website advertisements, ways to make money easily, miracle products, property offers, or simply lists of products on special offer.
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

D. Blogging

1. Please refer to 505.03 Social Media.

NOTE: If any of the above-prohibited uses is required for a legitimate business reason, it is management's responsibility to follow the exception process. All exceptions must be approved in writing from Chief Technology Officer or designee prior to use.

III. RESPONSIBILITIES

A. Employee Responsibilities:

1. Monitor personal use of the Internet, messaging, and other applications, to ensure that the City is being appropriately served.
2. Adhere to City standards as discussed in the language above.
3. Read and adhere to relevant City policies.
4. Obtain authorization from your supervisor before incurring charges; for example, downloading data or accessing a paid service.
5. Request Technology Services User Support (phone extension 8300) to download and install software unless expressed consent has been granted for employees to download and install software by Technology Services.
6. Preserve or archive any official City records stored on a personally-owned technology, communication device, or software in accordance with City records retention schedule and, when requested, turn these records over to the City Secretary's Office within 10 business days. NOTE: Failure to do so may result in penalties provided under state law for the employee, even if employment has ended during the records retention timeframe.

B. Management Responsibilities:

POLICY/ADMINISTRATIVE PROCEDURE/ADMINISTRATIVE DIRECTIVE (Continued)

TITLE: *ACCEPTABLE USE*	*REFERENCE NUMBER:* *506.01*

1. Ensure that the primary purpose of the use is to meet City business needs, and that relevant City standards are met.
2. Review and make decisions regarding the approval of all non-work-related broadcast announcements and acceptable uses for non-work-related use of City resources in compliance with applicable City policies.
3. Approve the use of personally-owned technology, communication device, or software for conducting City business and ensure that such use is in compliance with this directive.
4. Ensure employees using personally owned technology, communication device, or software are made aware of the public records requirements within this directive and the City's records retention schedule.

IV. ENFORCEMENT

In order to safeguard City resources, violators of this directive may be denied access to City computing and network resources and may be subject to other disciplinary action within and outside the City. Violations of this directive will be handled in accordance with the City's established disciplinary procedures. The City may temporarily suspend, block or restrict access to computing resources and accounts, independent of such procedures when it reasonably appears necessary to do so in order to protect the integrity, confidentiality, or availability of City computing and network resources, or to protect the City from liability. If violations of this directive are discovered, the City will take appropriate actions to resolve the issue and violators may be subject to disciplinary measures. If violations of this directive are discovered, which are illegal activities, the City may notify appropriate authorities. The City reserves the right to pursue appropriate legal actions to recover any financial losses suffered as a result of violations of this directive.

POLICY/ADMINISTRATIVE PROCEDURE/ADMINISTRATIVE DIRECTIVE (Continued)

TITLE: *ACCEPTABLE USE*	*REFERENCE NUMBER:* *506.01*

Agreement to Comply
Employee Acceptable Use Directive

All employees working at the City of Denton must submit a signed paper copy of this form. The City of Denton management will not accept modifications to the terms and conditions of this agreement.

_____

Employee's Printed Name

_____

Employee's Department

_____

Employee ID Number

I, the user, agree to take all reasonable precautions to assure that the City of Denton internal information, or information that has been entrusted to the City of Denton by third parties such as customers, will not be disclosed to unauthorized persons. At the end of my employment or contract with the City of Denton, I agree to return to the City of Denton all information to which I have had access as a result of my position with the City of Denton. I understand that I am not authorized to use this information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the City of Denton's *City Manager* who is the designated information owner. I have access to a copy of the City of Denton Acceptable Use Directive, I have read and understood the directive, and I understand how it impacts my job. As a condition of continued employment at the City of Denton, I agree to abide by the directive. I understand that non-compliance will be cause for corrective action up to and including system privilege revocation, termination of employment from the City of Denton, and perhaps criminal and/or civil penalties.

I agree to promptly report all violations or suspected violations of information security policies to the Chief Technology Officer.

_____

Employee's Signature Date