	City of Cedar Park Human Resources Policy Manual			
	Technology Use			
	Number: G-5	Revision: 1	Effective Date: 5/10/2018	Pages: 8

1.0 Policy

1.1 It shall be the policy of the City to provide to employees Technology Resources where determined to be of benefit to the City. The purpose of this Policy is to provide regulations to ensure the efficient and appropriate use of the City's Technology Resources.

1.2 This Policy applies to all City employees, including contract employees using City-owned or leased Technology Resources.

1.3 A user of City Technology Resources shall be responsible for the information contained in this Policy. The burden of responsibility is on the user to inquire as to acceptable and unacceptable uses prior to using City Technology Resources.

2.0 Procedure/Rule

2.1 Definitions.

2.1.1 *Smart Phones*. Devices that combine a cell phone with a hand-held computer, typically offering Internet access, data storage, and email capability.

2.1.2 *Technology Resources*. Any hardware, including personal computers, tablets, Smart Phones, mobile digital terminals (MDTs/Laptops), host systems, printers, scanners, flash/thumb drives, software, remote access, e-mail, text messages, Internet connection tools, and networks.

2.2 Confidentiality and Privacy.

2.2.1 All data that is composed, transmitted, or received via City Technology Resources in the transaction of City business is considered to be part of the official records of the City and is subject to Texas records retention laws and the Texas Public Information Act. **There is no expectation of personal privacy in the use of City Technology Resources**.

2.2.2 An employee's supervisor may monitor the activities of and inspect the City Technology Resources of a specific employee if the supervisor obtains concurrence from the Department Head or his/her designee and believes the employee to be in violation of this Policy. Additionally, the data that is composed via City Technology Resources may be viewed by the Information Services Department in the course of routine maintenance, or as needed for City administrative purposes, which includes investigations of possible violations of this Policy.

2.2.3 The City reserves the right to set permissions and accessibility rights as it deems necessary to all City Technology Resources. Except as pursuant to Section 2.2.2, no access shall be given to another employee's City Technology Resources without express permission from the appropriate Department Head or his/her designee, and such communication shall be communicated to the Director of Information Services.

An employee shall not access, copy, alter or destroy another employee's City Technology Resources without express permission from the Information Services Department and unless authorized or required to do so by law or regulation.

2.3 City Property. City Technology Resources are the property of the City.

2.3.1 An employee shall respect the legal protection provided by copyrights, licenses, and federal, state, or local laws and regulations. Copying of City-owned or licensed software or data to another computer system is prohibited without the prior written consent of the Director of the Information Services Department or his/her designee and the employee's Department Head.

2.3.2 No employee shall integrate personal Technology Resources containing inappropriate content with City Technology Resources.

2.3.3 An employee may bypass Net Mobility with approval from the Director of Information Services or his/her designee. However, no employee shall disable the Virtual Private Network technology (i.e., Net Motion Mobility) on City Technology Resources at any time.

2.3.4 Any employee who is issued a portable City Technology Resource shall possess that City Technology Resource whenever that employee comes to work during working hours.

2.4 Security ID.

2.4.1 The City's Technology Resources requires that each employee have a unique identity, referred to as a "User ID," which represents and identifies an employee in various system activities, provides access to certain software and data and associates the employee's own software and data with their identity. Assuming another employee's User ID, or assuming an anonymous identity, is expressly prohibited.

2.4.2 Each employee is responsible for any modification or access to system information made using his/her User ID. **An employee shall not share his/her passwords or leave any City Technology Resource unattended while logged on to City Technology Resources**. An employee should be aware that merely turning a Technology Resource off does not necessarily log the employee off the system.

2.5 Internet Use. Due to the very nature of Internet and online services, the City has no control over the content of messages or information postings on those services. The City reserves the right to use available technology to screen out information that may be offensive or not business-related, as determined by the City, although technology cannot block all sites that may contain offensive material, nor can the City prevent transmission and/or receipt of all offensive e-mail messages.

2.5.1 Right to Monitor. The City reserves the right to log, monitor and review all system and Internet connection and traffic information. If an employee receives offensive information, the employee should forward the information to the Information Services Department, who will attempt to minimize this type of activity.

2.5.2 Internet Connection. Internet use is provided through the use of a dedicated connection, and a firewall. Internet use outside of this configuration is prohibited unless specifically authorized by the Information Services Department and the employee's Department Head.

2.5.3 Pop-Ups. Offensive or obscene "pop-ups" should be reported to the Information Services Department.

2.6 E-Mail / Messages on Social Media.

2.6.1 Social Media Policy. All employees shall comply with the City's *Social Media* Policy.

2.6.2 City Records. Any email or message on social media sent or received through personal Technology Resources or City Technology Resources that is in the transaction of City business is considered a City record, and could be subject to disclosure to the public.

2.6.3 Professional Representation. When communicating with individuals, groups, or institutions when using City Technology Resources an employee does so as a representative of the City. An employee shall use these systems in a professional manner.

2.6.4 Accurate Representation. An employee shall represent him/herself according to his/her true and accurate identity in any electronic message, file and transaction at all times.

2.6.5 Personal Use. Incidental and occasional personal use of electronic messages may be permitted within the City, but such use shall not interfere with an employee's job performance.

2.7 Smart Phones. Use of Smart Phones includes both City-Issued Smart Phones and Personal Smart Phones used for City business.

2.7.1 Eligible Employees. Eligible Employees are employees:

A. Whose position is designated as an FLSA exempt position (i.e., not eligible for overtime compensation);

B. Whose job function requires extended time outside of assigned work areas and who must be accessible during that time;

C. Whose job function requires accessibility to a phone and email beyond scheduled or normal working hours; and

D. Who have permission to use and are using a City-issued Smart Phone or a personal Smart Phone for City Business pursuant to this Policy.

2.7.2 Use While Driving. No employee shall use a City-issued Smart Phone or a personal Smart Phone for City purposes while driving, unless the employee is using the Smart Phone with hands-free technology. In accordance with Texas Transportation Code Section 545.4251, as amended, drivers are prohibited from reading, writing, or sending electronic messages via a wireless communication device. This prohibition does not apply to employees operating authorized emergency or law enforcement vehicles while acting in an official capacity. (Also refer to *Use of City Property and Accident Reporting* Policy.)

2.7.3 Mobile Device Management. Each Eligible Employee shall have the City's Mobile Device Management (MDM) agent and related applications, and connect to the City's MDM system.

2.7.4 Operating System. Each Eligible Employee shall maintain the original device operating system and keep the device current with security patches and updates, as released by the manufacturer. The Eligible Employee shall not alter the security that is in place by the manufacturer as default (a.k.a., "jailbreak" or "root" the device) or install software that allows the Eligible Employee to bypass security features and controls. "Jailbroken" or "rooted" devices will immediately be disconnected from the City's network services.

2.7.5 Passwords. Eligible Employees shall password protect his/her device, and shall keep that password confidential.

2.7.6 City-Issued Smart Phones. Issuance of a City-issued Smart Phone device to an Eligible Employee is at the discretion of the Eligible Employee's Department Head or her/his designee. The Department Head or his/her designee reserves the right to recall/disconnect City-issued devices if she/he determines that such use is not in the best interested of the City for such reasons, including:

2.7.6.1 Violation of this Policy;

2.7.6.2 Non-use or limited use of the device;

2.7.6.3 Excessive personal use of the device that interferes with job performance; or

2.7.6.4 Budgetary constraints.

2.7.7 Personal Smart Phone Used for City Business.

2.7.7.1 Eligible Devices. A list of approved devices is listed on IS's intranet site. Devices not on the approved list must be evaluated by the Information Services Department for compatibility with the City's Technology. The device must be compatible with City services (i.e. email, calendar, contacts synchronization). The employee is responsible for ensuring compatibility. The device must be able to receive phone calls and data transmission through-out Cedar Park and the surrounding areas and a majority of the state of Texas. The phone number associated with the device must have an Austin area code (512 or 737).

2.7.7.2 Participation in Reimbursement Program Discretionary. Participation in the reimbursement program is discretionary. The City Manager or her/his designee reserves the right to cancel participation in the reimbursement program if she/he deems that such participation is not in the best interest of the City for such reasons, including:

A. Violation of this Policy;

B. Non-use or limited use of the device for work purposes;

C. Excessive personal use of the device that interferes with job performance; or

D. Budgetary constraints.

2.7.7.3 Use. Eligible Employees who use personal devices for City business shall:

A. Conduct City business only on City accounts downloaded onto the personal device;

B. Retain an active phone and data plan with enough capacity to adequately conduct City business;

C. Notify the Eligible Employee's Department Head and Human Resources if the Eligible Employee's phone number changes; and

D. Submit a copy of the phone and data plan charges annually to the Finance Department.

2.7.8 Separation of Employment. The City reserves the right to remove all City software, files, data, and configurations from the Eligible Employee's personal smartphone upon the Eligible Employee's separation from employment.

2.8 Viruses. The City desires to protect its Technology Resources from both the intentional and unintentional introduction of any computer virus. Therefore, an employee shall also practice safe computing, which includes:

2.8.1 Exercising care when receiving messages through the internet, software, or hardware from a third party; and

2.8.2 Immediately report any suspicions of viruses to the Information Services Department.

2.9 Purchasing and Upgrade Processes.

2.9.1 Purchase. To provide the most cost-effective and efficient service, any hardware or software acquisition, whether new or upgrades, shall be coordinated with the Information Services Department and the requesting department before a purchase is made. If such a purchase is not coordinated with the Information Services Department, a system may not be supported and may be removed from service.

2.9.2 Installation. The installation of Technology Resources shall be made with assistance from the Information Services Department.

2.9.3 Storage of Licenses. Physical software licenses and disks should be stored with the Information Services Department, unless otherwise directed by the Information Services Department.

2.10 Prohibited Uses. In addition to the regulations specified in this Policy, an employee is specifically prohibited from using the City's Technology Resources in any manner identified in this section. Specific exemption to these prohibited uses may be made for Police Department investigations with the approval of the Chief of Police or his/her designee. Such prohibitions include, but are not limited to:

2.10.1 Use for any purpose that violates any City, state or federal law;

2.10.2 Destruction or damage to City Technology Resources;

2.10.3 Use for private business, commercial purposes or personal financial gain, including external consulting, or commercial advertising;

2.10.4 Use that produces an adverse effect, disrupts the work environment, or interferes with workplace operations of the City;

2.10.5 Use of City Technology Resources for purposes other than those intended by the department authorizing access, including allowing access by unauthorized persons;

2.10.6 Personal use that is inappropriate or more than incidental or occasional;

2.10.7 Storage of information that is private or personal and affects the performance of the Technology Resource;

2.10.8 Downloading or use of applications, including games, other than those approved for City information management purposes;

2.10.9 Viewing, sending, copying or soliciting of sexually oriented messages or images;

2.10.10 Accessing internet sites which are "adult oriented" in nature, or which offer gambling services, or which contain obscene content of any nature;

2.10.11 Use to defraud, threaten, libel or harass others, including transmission of offensive or harassing statements or images that disparage others based on their race, national origin, sex, sexual orientation, age, disability, religious beliefs, political beliefs, or any other classification protected by law;

2.10.12 Impersonation of any person or communication under a false or unauthorized name;

2.10.13 Inappropriate mass mailing, "spamming" or "mail bombing";

2.10.14 Tampering with any software protections or restrictions placed on computer applications or files or attempting to circumvent local or network system security measures;

2.10.15 Knowingly or maliciously introducing any invasive or destructive programs into City Technology Resources or intentionally developing programs designed to harass other users or infiltrate and/or damage City Technology Resources;

2.10.16 Attempting to modify, damage, interfere with or disrupt the operation of City Technology Resources;

2.10.17 Use or fundraising, partisan politics or public relations activities not specifically authorized by the Department Head or designee and not related to City activities;

2.10.18 Intentionally seeking information or security access rights on, obtaining copies of, or modifying files or data without proper authorization; or

2.10.19 Intentionally copying or printing any software, electronic file, program or data using City Technology Resources without specific authorization by the Information Services Department Director or his/her designee and the Department Head or his/her designee.

3.0 Enforcement. An employee who violates this Policy shall be subject to revocation or suspension of user privileges and/or disciplinary action, up to and including termination of employment.