INFORMATION TECHNOLOGY

Department of Information Technology

City of Seguin IT Policy

September 2019

Version	Title/Modifications	Date Modified	Changed by:	Approved by:
1.0	Document creation	4/22/2019		Shane McDaniel
1.0	Document approved	9/24/2019	Andy Quittner/Shane McDaniel	Douglas Faseler

Table of Contents

City of Seguin Policies Governing Use of Computer Hardware, Software, City Networks and Social Media

I. Purpose

This policy serves to protect the security, integrity and acceptable use of the City of Seguin's (hereinafter the "City") technology systems and City owned technology assets by educating, employees and other users regarding appropriate and safe use of technology resources. City technology systems, network resources, on premise software, cloud assets and hardware including but not limited to desktop computers, laptops, iPads and other mobile resources (collectively "City IT resources") constitute expensive and valuable assets of the City. The City is obligated to protect these assets and the entirety of the City's virtual enterprise as to ensure use of these assets are lawful, appropriate, secure and in the best interest of the City.

As a governmental entity the City's IT resources are subject to the Texas Open Records Act. As such the City reserves the right to inspect and retrieve any data, email, social media content, files, settings or any other aspect and/or access made by a City owned or subsidized technology device and will do so on an as-needed basis as determined by the City Manager, City Attorney, Director of IT or department heads.

This policy supplements the rules and policies in the City of Seguin Employee Handbook, the Seguin Code of Ethics and any other policies, procedures, rules and directives as adopted and applied to respective duties and responsibilities by the City. An employee's access to and use of City owned and provided IT resources, technology platforms, social networking and other websites is subject to this policy in addition to other adopted City employee policies.

All individuals utilizing City IT resources are responsible for reading and following technology best practices and directives that may be distributed as needed by the IT department regarding appropriate measures to protect various City technology assets.

II. Privacy

For users of City IT resources there is no guarantee or expectation of personal privacy. As a government entity the City of Seguin is subject to the Texas Open Records Act. The Texas Open Records Act applies to government information without respect to the method of dissemination or storage to include dissemination from personal IT resources. Decisions as to information private or otherwise, held, stored or disseminated from City or personal IT resources can be disclosed to the public depends upon the opinion of the City Attorney and/or Texas Attorney General's Office.

All users of City IT resources are to understand that under appropriate circumstances all information, both personal and business, may be subject to review and potential disclosure. Employees should keep in mind that any personal comments or information contained within a communication related to City business is potentially subject to disclosure regardless of whether the personal information is related to the primary business being communicated.

III. City Owned Private Network

No employee or other person shall install, connect or move any technology device within or onto the City owned communications network under any circumstance; only IT Department staff are authorized to perform these functions. Under no circumstances is an employee, contractor or third party authorized to install any device or software intended to monitor, capture or eavesdrop upon any portion of data traversing the City network without prior knowledge and

authorization from the IT Department except for the IT Department staff acting within the parameters of assigned duties.

No employee will permit any third party to connect any device to an Ethernet jack or wireless service in a City owned or operated facility without the consent of the IT Department or designee unless specifically authorized to allow such a connection. The exception to this is the City hosted guest Wi-Fi networks annotated and made available as ***"CityofSeguin-Guest, CityofSeguin-Presenter, Seguin-Complex-Guest and Library Public Wi-Fi"*** in City facilities.

No employee or vendor shall install or operate any technology hardware, software or service that can implement redirection or proxying network traffic to or from other networks via disguising the source of a network transmission. *Any hardware or software technology to be used in conjunction with the City owned private network must be approved and authorized by the IT Department.*

IV. Internet Acceptable Use

All employees are prohibited from accessing any streaming media programs (including streaming on your cellphone, multimedia or other mobile devices through City provided Wi-Fi), feeds, material and content without the authorization of the City Manager or Director of IT unless the subject matter being streamed is necessary to fulfill one's job responsibilities. No streaming media sites are to be accessed, nor are any streaming media programs or applications to be downloaded, installed and/or operated by end users utilizing City provided computers, servers, systems and/or networks without the expressed written consent or the City Manager or Director of IT.

Employees are also prohibited from accessing media streams from such Web sites as Google Video, iFilm, YouTube, Netflix, Hulu, Amazon, Sling and DirectTV Now among others unless the subject matter being streamed is necessary to fulfill one's job responsibilities. Streaming media programs and devices prohibited from operation within the organization or on any organization equipment or network (unless used for expressly permitted activities) include but are not limited to:

A. Internet Radio (Pandora, XM, Sirius, iHeartRadio, Spotify, Apple Music, Amazon Music or others);

B. Video streaming sites (YouTube, Netflix, Hulu, iTunes, Google Play, Sling, DirectTV Now and others);

C. Messaging Apps (Snapchat, WhatsApp, Facebook Messenger, Slack and others).

Violating the streaming media policy could result in disciplinary action up to and including termination of employment in accordance with the City's established policies and procedures related to discipline and discharge.

V. Offensive and Inappropriate Material

Users of City IT resources are not to access or distribute any material that could be considered inappropriate, offensive, unprofessional or disrespectful to others internal and external to the City of Seguin. While it is impossible to list every form of such material some clear examples include but are not limited to pornography, sexually explicit material, racial slurs and material related to terrorism or other criminal activity.

Employees should discuss questions concerning inappropriate or offensive material with their supervisor or director. Any employee found in violation of this policy may result in disciplinary action up to and including termination and possible prosecution under applicable local, state and federal laws. The City of Seguin will take every step necessary to include legal measures to protect its employees and assets.

The display or email transmission of any sexually explicit image or document on any City IT or personal resource used on City premises is a violation of City policy. Sexually explicit material may not be viewed, archived, stored, distributed, edited, emailed or recorded using City IT resources. The display of any materials considered to be offensive or inappropriate that advocate intolerance for others is a violation of City policy.

The City may use independently supplied and internally developed software and data to identify inappropriate or sexually explicit Internet sites. The City may block access from within the network to any site determined inappropriate. If an employee finds themselves connected incidentally to a site that contains sexually explicit, offensive or otherwise inappropriate material they must disconnect from the site and contact the IT Department immediately.

Employee posts or actions resulting in an inordinate amount of inbound email to include Spam, flames or mail bombs may lose their access to the Internet and/or email. Use of the Internet that interferes with the work of other City employees, contractor's other business associates or clients is prohibited.

VI. Security

The security policy applies to all information owned, obtained, created or maintained on City IT resources or technology services extended to personally owned devices (email for example). These standards apply equally to all users of City IT resources and the content stored within until the time of said content is destroyed, erased or permanently transferred to a third-party external entity. Security practices and policies shall be reviewed on a regular basis with new policies distributed to users upon approval by the City Manager and HR.

It is not the intent of the City to hinder employee operational workflow, processes, tasks or day to day responsibilities with superfluous end user security requirements. Malicious actors are continuously seeking virtual and physical vulnerabilities to gain access into private domains for malevolent intent. The City of Seguin security guidelines were established to reduce and eradicate said vulnerabilities into the City's technical environment as to keep those that desire to inflict disruption and harm to the City's technical enterprise from doing so. Every City employee plays a significant role in protecting the City's physical and technical environments from being compromised. It is the expectation of City Management that all City employees will adhere to current and future security guidelines established.

Employee/End User Security Awareness Guidelines:

A. Security controls placed on City IT resources may not be bypassed or disabled. Attempts to bypass or disable security controls may result in disciplinary action as set forth in this policy;

B. Security awareness needs to be continually emphasized, reinforced, updated and validated. Directors and supervisors shall help to ensure that their employees are following proper security protocols;

C. All users are responsible for managing their use of City IT resources and are accountable for their actions relating to security. Users are also equally responsible for reporting any suspected or confirmed violations of this policy to their supervisor and/or the IT Department;

D. Passwords, Personal Identification Numbers (PINs), access controls and other computer systems security procedures and devices shall be protected by the user from use by or disclosure to any other individual or organization. All security violations including lost or stolen passwords, badge access cards or PINS shall be immediately reported to the employee's supervisor, the IT Department or the City Manager;

E. Users are not permitted to share or let others including but not limited to co-workers and family members use their password or PIN for access to City IT resources. Allowing access to City IT resources or use of passwords and other security measures by unauthorized users or by direction of supervisors/directors may result in disciplinary action as set forth in this policy;

F. Information access authority for each user shall be reviewed on a regular basis as well as with each job status change such as transfers, promotions, demotions or termination of service. All requests for a change in access shall be submitted to the IT Department by an employee's Director via a helpdesk ticket;

G. When circumstances merit confidentiality (for example customer personal data), all users have the duty to keep such information confidential and secure. The fact that the data may be stored electronically does not change this requirement. The type of information or the information itself is the basis for determining whether the data must be kept confidential and secure;

H. City owned computers and mobile devices must be locked at all times if the user steps away and cannot maintain continual sight on their respective workspace. Failure to meet this requirement may result in shorter computer lockout times assigned to the device as to prevent the City owned asset from unauthorized access;

I. All computer software programs, applications, source code, object code, documentation and data shall be guarded and protected as if it were the City of Seguin physical property. Users may not copy or use City supplied software on any other computer, smart phone or other electronic device without the consent of the IT Department. The release of computer programs or data, including email lists and departmental telephone directories to other persons or organizations must comply with all City legal and fiscal policies;

J. All departments must carefully assess the risk of unauthorized alteration, unauthorized disclosure or loss of the data for which they are responsible and ensure that City IT resources are protected from damage monetary or otherwise. Information systems must have appropriate backup and contingency plans for disaster recovery based on risk assessment and business requirements;

K. On termination of employment users must surrender all property owned and/or managed by the City. This includes all City owned technology hardware and software as well as badges for access into City facilities. All security policies apply to and remain in force in the event of a terminated relationship until such surrender is made;

L. Approval must be obtained from the IT Department before connecting a device to the City's private network. The Director of IT or assigned designee reserves the right to remove any network device that does not comply with standards or is not considered to be adequately secure;

M. Computer systems or associated equipment used for City business that is conducted and managed outside of City control must meet contractual requirements and be subject to monitoring. External access to and from City IT resources must be approved prior to access by the Director of IT or an appointed designee.

Security Incidents:

As a means to eliminate potential cybersecurity vulnerabilities if malicious software and/or traffic is found on a City owned network or a device utilizing City provided technology servicers or platforms, to include personal devices on the City's wireless guest network, the City reserves the right to permanently block that device from use of City provided technology resources.

In the case of a City employee or citizens utilizing a personal device on City provided resources, the owner of the blocked device may formally request that the City's IT Department unblock said device. It will be at the discretion of the Director of IT or a designated appointee as to if the device will be unblocked and allowed future use of City provided technology resources. A blocked user may make a formal appeal to the City Manager if they do not agree with the Director of IT's or the appointed designee's decision regarding their personally owned device. Incident response and any subsequent actions will be on a case by case basis.

VII. Audio/Video Surveillance

The City of Seguin reserves the right to place audio/video monitoring and/or recording equipment on its premises where necessary and appropriate in accordance with this policy. This policy applies to all property owned or controlled by the City of Seguin and/or its representatives. Applicable law may supersede this policy. This policy does not apply to covert cameras used by law enforcement agencies for law enforcement purposes. City of Seguin employees should not expect privacy in work-related areas because of this policy.

Video Surveillance and Audio Monitoring Equipment

A. The acquisition and installation of audio/video monitoring and/or recording equipment must be coordinated and approved through the City Manager and Director of IT;

B. The City of Seguin shall not make video or audio recordings or conduct surveillance without the proper and legal acknowledgments and/or postings as required by law, policy, rule or regulation;

C. Video monitoring of currency handling areas may be constant as to protect employee and customer interests;

D. False, empty, dummy or inactive cameras are prohibited unless authorized by the City Manager and may result in investigation and prosecution;

E. Employees are not to record video interactions, of professional or personal nature, at any time or for any reason on a personally owned device.

Video Surveillance

In order to promote the safety of employees and visitors as well as the security of its facilities the City of Seguin may conduct video surveillance of any portion of its premises at any time with the exception of private areas for restrooms, showers and dressing rooms. Privacy of employees will be respected to the extent possible. Reasonable belief of on-site drug use, physical abuse, theft or similar circumstances would be possible exceptions. Legal advice will be sought in advance to rare cases where non-work area privacy must be compromised.

Audio Recording/Monitoring

A. Members of the management team or their designee may record and/or listen in on customer service lines to ensure employees are being respectful and responsible to customers or for other legitimate business purposes. Calls may also be recorded and/or monitored for training purposes to critique customer service skills and provide feedback for job performance as needed;

B. Employees may be monitored at any time during business calls without notification. Each employee's written acknowledgment will be obtained prior to his/her commencing employment and a signed copy of this policy will be placed in the employee's file. In addition, customers will also be notified of possible monitoring;

C. A continuously excessive level of non-business-related phone calls is a basis for disciplinary action;

D. Employees are not to record audio interactions, of professional or personal nature, at any time or for any reason on a personally owned device.

Review of Audio/Video Surveillance Recordings

Only authorized personnel shall be allowed to review the audio/video surveillance recordings. The authorized personnel will be designated in the request for audio/video surveillance equipment through the City Manager or a designee, Director of IT or HR Department. The City Manager and/or HR Director will make the final determination as to who may view the audio/video surveillance recording.

Audio/Video Monitoring Storage

The recording media will be on a reusable single source schedule as designated by the IT Department and will be retained in accordance with regulations for government mandated records retention requirements. Recordings not covered by the records retention policy will be retained only if required for operational necessity.

Release of Recordings

Audio or video recordings will not be viewed or released outside of the organization unless required by criminal proceedings, the Texas Public Information Act, law, regulation or as deemed appropriate by the City Manager.

Destruction or Tampering with Audio/Video Recording Equipment

Any person who tampers with or willfully destroys any audio/video monitoring and recording equipment or recorded video may be disciplined up to and including termination.

VIII. Software

To prevent cybersecurity malware from being transmitted through City IT resources *unauthorized downloading of any non-approved software is strictly prohibited.* Only software registered and/or approved through the IT Department may be downloaded without authorization; any questions concerning software should be directed to the IT Department. Approval for new software must be attained from the director of the requesting employee's department and a help desk ticket submitted confirming department head approval.

All commercial software to include freeware and/or shareware used on City IT resources must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product. Personnel must abide by all license agreements and must not illegally copy licensed software. The IT Department reserves the right to remove any unlicensed software from any City owned or operated computer system.

Departments shall engage the IT Department at the onset of any project to acquire computer hardware or to purchase or develop computer software to be used in conjunction with the City's network enterprise. The costs of acquisitions, development and operation of computer hardware and applications must be authorized by the respective department head in conjunction with the City Manager and the Director of IT. The requesting department must act within their delegated approval limits in accordance with the City's authorization policy.

For all software contained within or transmitting through the City's private network and/or City IT resources the IT Department will require adequate access controls to monitor systems, security or to protect data and programs from misuse in accordance with the needs defined by departments, the equipment or under the software license.

All technology systems contracts, leases, licenses, consulting arrangements or other agreements must be authorized by the City Manager and the Director of IT in conjunction with the City's Legal Counsel. The purpose of which being to advise vendors of the City's retained proprietary and rights with respect to its information systems, programs, and data requirements for computer systems security to include data maintenance and retrieval.

The IT Department reserves the right to remove any non-business-related software or files from any City owned IT resource. Examples of non-business-related software or files include but are not limited to games, instant messengers, music and video files, image files, freeware and/or shareware.

IX. Copyright and License

Employees are to respect copyrights and licensing to software and other copyrighted information. Software protected by copyright must not be copied into or from City IT resources except as specifically stipulated in the City's license agreement or as otherwise permitted by copyright laws. Copying or downloading software from City resources is not authorized, to include for use for work at home, without express permission by the City Manager or Director of IT.

All other copyrighted information including but not limited to music, video, text and images retrieved using City IT resources must be used in conformance with applicable copyright and laws. City related business use of copyrighted material must be properly attributed.

X. Email, Electronic Files and Documents

All information stored and/or disseminated on or through City IT resources is potentially subject to the Texas Open Records Act regardless of whether the information contains personal or non-City related data. There is no expectation of personal privacy with any City owned technology device, including use for personal business. The use of electronic communication tools may be monitored to fulfill open records requirements, complaint, investigation requirements or City related litigation. Department heads responsible for the custody of electronic records shall be responsible for proper authorization of record utilization, the establishment of effective use and reporting of performance to the IT Department.

Leveraging City IT resources to send or reply to chain letters, hoaxes or virus warnings is prohibited. If an employee receives a chain letter or virus warning it is not to be forwarded. If an employee receives notice regarding a supposed virus or code threat report the threat immediately to the IT Department.

When using email to communicate municipal business City employees, interns or other users of City IT resources are required to use an official City owned email account issued by the City. Private email accounts may not be used to transact or communicate City business. If the City email system is unavailable and a private email account must be used, all email sent or received involving City matters must be forwarded immediately to the appropriate City email account as soon as the City email system is available.

Employees may use City IT resources for non-work/personal use or browsing during mealtime, breaks or outside of work hours provided that all other Internet usage policies are adhered. Personal use of the Internet and email must not be in connection with any personal business activity, the business of any other corporation or firm, consulting effort or similar profit venture. Using City IT resources to access the Internet or send email for solicitation of money, partisan or political purposes, social or religious causes is strictly prohibited.

Do not place any material on the Internet or send email that could be considered inappropriate, offensive or disrespectful to others and do not access or forward such material. Employees with Internet access may not use City IT resources to access non-business-related file exchange or sharing services. Employees may not use City IT resources to participate in online gambling.

XI. Representation of the City of Seguin

Each employee using City IT or personal resources when discussing City matters shall identify themselves honestly, accurately and completely to include one's City affiliation and function where requested. A City employee must never masquerade as someone else. Forgery or attempted forgery of email messages and use of pseudonyms is prohibited.

Any false representation of authority or engagement in unauthorized business is strictly prohibited both during and outside of business hours. Only those employees or officials who are duly authorized to speak to the media, to analysts or in public gatherings on behalf of the City may speak or write in the name of the City to any newsgroup or chat room. Other employees may participate in newsgroups or chats during business when relevant to their duties but do so as individuals speaking only for themselves. When an individual participant is identified as an employee or agent of the municipality the employee must refrain from any unauthorized political advocacy and/or apparent endorsement by the municipality of any commercial product or service.

Email addresses may satisfy the requirement for a legal signature. It is the responsibility of the employee to avoid creating unwarranted contractual obligations. In any electronic communication in which the possibility of contracting exists a disclaimer must be included indicating that official approval must be obtained prior to agreement.

The City does not accept responsibility for the personal opinions expressed by its employees. Employees with Internet access must take care to understand the copyright, trademark, libel, slander and public speech control regulations so that use of the Internet does not inadvertently violate any laws which might be enforceable against the municipality.

XII. Social Media

This policy outlines the protocol and procedures for the use of social media to publicize official City news, services and events. In addition, this policy provides guidance to City employees concerning their use of and responsibilities regarding social media on City IT resources.

For the purposes of this policy social media is defined as official City websites along with all forms of online community activities such as online social networks (e.g., Facebook), professional networking sites (e.g., LinkedIn), message boards (e.g., Twitter), video sharing (e.g., YouTube), blogs, wikis, chat rooms and online forums. Personal use of social media shall be limited to mealtime, breaks or outside of work hours.

The ***official*** voice of the City shall be the City's website ***www.seguintexas.gov***. All City existences on social media sites or services are considered an extension of the City's information networks and are governed by the rules and regulations set forth in this policy and any other applicable policy to include any future changes made. Official social media sites/pages representing the City will be the property of the City.

Accounts must be registered through the Public Information Officer (PIO). The PIO will secure approval from the City Manager before establishing accounts as needed.

The Public Information Officer will be responsible for the oversight of the City's social media formats to include:

A. Authorizing social media accounts;

B. Maintaining a list of social media domains as well as usernames and passwords;

C. Monitoring social media activity to verify that content is compliant with the City's goals, objectives and ethical conduct policy;

D. Access to all administrative rights and privileges of all social media domains and accounts.

For acceptability the content of the social media must contain:

A. Information about City events, activities or issues tied to something funded, operated, managed, etcetera by the City;

B. Positive aspects of the City of Seguin;

C. Reflect the goals and purpose of the account.

Postings to City social media sites must be respectful and shall NOT contain any of the following:

A. Comments that are not topically related to the post commented upon;

B. Comments in support of or opposition to political campaigns, candidates or ballot measures;

C. Profane language or content;

D. Content that promotes, fosters, or perpetuates discrimination on the basis of race, creed, color, age, religion, gender, marital status, national origin, physical, mental disability or any other category protected by federal, state or local laws;

E. Sexual content or links to sexual content;

F. Solicitations of commerce;

G. Conduct or encouragement of illegal activity;

H. Information that may compromise the safety or security of the public or public systems;

I. Content that violates a legal ownership interest of any other party including the disclosure of private or confidential information;

J. Information about current or pending claims and litigation involving the City;

K. The intellectual property of others without written permission;

L. Photographs of employees or members of the public without consent or publicly posted notice provided.

The City website will remain the official location for content regarding City business, services and events. When possible, links from social media sites will be used to direct users back to the City's website for more information. Only designated employees will have authority to change content of the social media site.

Communications through social media is public record; posts by City departments, employees and any outside feedback will be part of the public records for the City. The PIO will be responsible for establishing guidelines for maintaining and storing copies of the content posted in order to comply with the Texas Public Information Act.

Content posted by outside contributors and not officially posted by the City do not constitute an endorsement or representation on the part of the City. The City also reserves the right to block any users that violate these guidelines from accessing the City's social media sites.

If a question arises regarding the use or posting of confidential information on a social media site, the matter will be referred to the City Attorney for review. The information shall not be posted, or if already posted will be removed immediately until an opinion is rendered by the City Attorney. The City Manager or designee reserves the right to restrict or remove any information on the social media site that he/she does not believe serves in the best interest of the City.

Each official City social media page will include a disclaimer that contains wording similar to:

"The City of Seguin maintains this social media site/page to provide information and promote City programs, services, policies and objectives. It is the City's goal to keep the most current and accurate information available to the public on this site, however, varying events can occur that could affect the timeliness of the information and the accuracy of the content. Comments posted on this site by "friends," "fans," or "followers" will be monitored and any postings or comments that are disrespectful, offensive, dishonest, or do not accurately reflect the views, values or objectives of the City of Seguin will be deleted without notice. This site/page may contain links to other Internet sites and resources as a convenience to the viewer. Linked sites/pages are not under the control of nor maintained by the City of Seguin and the City is not responsible for the content of these sites. The inclusion of a linked site/page does not constitute an endorsement or promotion by the City of Seguin."

Authorized Publisher and Internet Use of Social Media

As a governmental entity the City expects its employees to exercise discretion when they share opinions, insights, experiences and perspectives on social media. City employees who choose to utilize social media need to understand what is recommended, expected and required when discussing City-related topics, whether at work or on their own time. Depending on position employees are considered by the public as a Seguin employee/representative at all times.

The City of Seguin acting through its City Manager has an overriding interest and expectation in deciding who may "speak" and what is "spoken" on behalf of the City of Seguin on social media sites.

Wherever possible links to information should direct users back to the City's official website for information, forms, documents or online services necessary to conduct business with the City. For any official Seguin social media site, the use of disparaging remarks and personal email addresses is prohibited.

Departments that use social media are responsible for complying with applicable federal, state and City laws, regulations and policies. This includes adherence to established laws and policies regarding copyright, records retention, the Americans with Disabilities Act and Texas Public Information Act (TPIA), retention laws and policies, the First Amendment, privacy laws and information security policies established by the City.

The City regards blogs and other forms of online discourse as primarily a form of communication and relationship among individuals. The City does not permit employee bloggers from working anonymously or using pseudonyms or false screen names in blogs, wikis or other forms of online participation that relate to the City, its business dealings or issues with which the City is engaged. If an employee blogs about their work for the City they are to use their real name, be clear who they are and identify that they work for the City. Participation online results in a user's comments being permanently available and open to republishing on other media outlets. Users should be aware that libel, defamation, copyright and data protection laws apply.

The lines between public, private, personal and professional communications are blurred on online social networks. By identifying as a City employee within a social network an employee is now connected to colleagues, managers and City clients. Employees should ensure that content associated with them is consistent with their City work. If an employee has recently joined the City, they are to ensure that they update their social networking content to reflect City guidelines and this policy.

Whenever expressing personal opinion, particularly on personal websites where an employee may be known as a City employee, a disclaimer must be used. If an employee publishes a blog or some other form of social media, they are to make it clear that what they say is representative of their views and opinions and not the views and opinions of the City. At a minimum in the employees blog the following standard disclaimer should be included:

"The postings on this site are my own and don't necessarily represent positions, strategies or opinions of the City of Seguin."

The standard disclaimer set forth in the above paragraph does not by itself exempt City supervisors and executives from responsibility when blogging or participating in social media sites. By virtue of their position, supervisors, managers and executives must consider whether personal thoughts they publish may be misunderstood as expressing the City's positions. Social networking sites are not the place to communicate City policies, procedures and business to their employees.

For the City's protection and that of respective employees it is critical that everyone shows proper respect for the laws governing copyright and fair use of copyrighted material owned by others to include the City. Employees are to be certain of ownership rights or the right to use all material that is placed on a City social media site including photographs, clip art and music/video clips. Attribution of ownership must be included in the publication of any photograph, clip art, music, video or document that is not created by the City or a City employee.

Remember that the City is a regional organization whose employees and clients reflect a diverse set of customs, values and points of view. Employees must not distribute ethnic slurs, personal insults, obscenity, etcetera or engage in online conduct that might be considered objectionable or inflammatory. An online audience is to be treated with the same respect as an in-person conversation.

If an employee is about to publish something that makes them even the slightest bit uncomfortable, review the above suggestions. If the employee is still unsure and it is related to the City, they should discuss it with their supervisor, manager or director before publishing. Ultimately employees are solely responsible for what they post or publish on any form of online social media.

Use of Social Media at Work

Work-related social media access by employees while on duty utilizing City property will be subject to the rules and guidelines set forth by the City's HR Department. Personal use of social media by employees while on duty utilizing

City property will be subject to the same rules and guidelines. *Media inquiries generated on social media sites should follow the protocols adopted by the City.*

The City reserves the right to monitor employee use of social media sites accessed during work hours on City IT resources. Users should have no expectation of privacy or confidentiality when leveraging these resources. Employees may not ignore copyright laws, cite or reference sources inaccurately. Plagiarism is prohibited.

All information published on social media sites must comply with the City's privacy and/or data policies. This includes comments, pictures, video, audio or any other multimedia posted on social networking sites, blogs and forums. Employees are discouraged from discussing information about City employees, citizens, vendors, issues, business or legal matters without expressed written consent to do so.

All City-related communication through social media outlets should remain professional in nature. Incomplete, inaccurate, inappropriate, threatening, demeaning, harassing or poorly worded postings may be harmful to other employees, damage employee relationships, create hostile working environments, violate City policies or harm the City's reputation. Such wording will be removed by the PIO at their discretion. Employees bear full responsibility for the material they post on social media sites. Inappropriate usage of social media can be grounds for disciplinary action up to and including termination of employment.

The City reserves the right to remove content that is deemed in violation of this policy or any applicable law. Violations of this policy may result in immediate revocation of any and/or all electronic communications access, user privileges and may be grounds for disciplinary action up to and including termination. Certain violations could result in civil or criminal liabilities.

Use of Social Media at Home

While the City encourages employees to enjoy and make good use of their off-duty time, certain activities on the part of employees may become a concern if it impairs the operation of the City or the work of any employee. Harassing, demeaning or creating a hostile work environment for any employee, disrupting the smooth and orderly flow of work within the office or harming the goodwill and reputation of the City among its citizens or in the community at large will not be tolerated. In the area of social media employees may use such media outside of work as long as such use does not produce the adverse consequences noted above. For this reason, the City reminds its employees that the following guidelines apply to their use of social media both on and off duty:

A. Information that is published on personal online sites should never be attributed to the City and should not appear to be endorsed by or originated from the City;

B. Employees engaging on personal social media platforms are prohibited from using their City email account without prior approval or the City's name, logos, pictures of the employee in a City uniform, incorporate the City in their identity (e.g., username, "handle", screen name or profile picture), nor should they speak as a representative of the City;

C. Any person identified as an employee of the City on a publicly accessible site is expected to maintain a positive online image that is consistent with the City's goals and objectives;

D. Employees that choose to list their employment affiliation on public websites should regard all communication on that site as professional;

E. Employees that contribute to a public site or blog and identify themselves as a City employee are asked to provide a clear disclaimer that their views are not endorsed by the City and are their beliefs alone;

F. Relationships with other City employees established outside of work on social media sites may have an adverse effect on work relationships. Employees shall not use social media outside of work to tease, harass, bully or in act in a manner that would adversely affect a coworker. Employees should be mindful of this possibility;

G. Posts should not disclose private or confidential information including posting photographs of fellow employees or citizens without their permission.

XIII. Mobile Technology

The purpose of this policy is to ensure that privacy, security and legal issues concerning the use of mobile technology is addressed and that a policy is formally established to define an appropriate procurement procedure and use of these services and equipment. This policy covers any mobile technology device issued by the City of Seguin to include personally owned cell/smart phones which may be used by employees for City business purposes.

City-issued mobile devices and all information created and stored therein are the property of the City. For the protection of the organization and its employees City staff issued mobile devices are required to review and abide by this policy. This policy applies to all employees, departments and full-time, part-time, contract, temporary or seasonal hires. Departments can implement more restrictive conditions on the use of mobile technology than those defined within this policy.

Software services, cloud technology and the data stored therein provided by the City and extended to personally owned smart phones and other mobile devices are the property of the City. Access to any City provided cloud technology authorized for personally owned smart phones and mobile devices can be revoked without notice at the discretion of the City Manager, Director of IT, HR Director or City Attorney. City technology services and data extended to personally owned smart phones and mobile devices are subject to the Texas Open Records Act.

City owned mobile technology is defined as any mobile technology device purchased by the City wherein the City is holistically responsible for paying the billed cost of that device's usage. Examples of mobile technology includes but is not limited to cell/smart phones, iPad's, SIM cards, jetpacks, mobile hotspots or tethering devices. City employee is defined as any employee (including permanent, full-time, part-time, and seasonal employees) of any City department. Personal use is defined as usage for purposes other than City business purposes. Smart phone pertains to cell phone devices that integrate the functionality of a mobile phone, email, web access, data plan and other functions.

Appropriate Use

Employees are expected and obligated to leverage good judgment and care when using City owned mobile and cellular devices. Access to these technologies is made available to City employees for the purpose of providing an effective method to communicate and increase productivity. Employees are permitted limited use for personal needs as long as it does not interfere with official business, result in the loss of employee productivity or increase the City's financial burden for said device. Personal use of City technology must be kept to the minimum amount of time needed to address a situation. Excessive use will be determined on a case-by-case basis.

Security

To prevent inadvertent downloading of imbedded malicious software into the City owned private network mobile devices to include both City provided and personally owned cell/smart phones, iPads and/or rogue USB devices

(flash drives, external hard drives, etc.) are not to be plugged into or connected to City owned and provided desktop and/or laptop computers at any time. This is to include physical (USB, USB-C) or wirelessly connectivity via Bluetooth technology.

Prohibited Uses

City owned mobile device users are prohibited from using City owned devices for the following activities:

A. Transmitting or downloading any material or messages in violation of Federal, state, ordinance, regulation or City policy including but not limited to sexually, racially or ethnically offensive comments, threats, jokes or slurs;

B. Distributing sensitive or confidential information;

C. Using City provided resources to accomplish personal gain or to manage a private business;

D. Downloading or distributing copyrighted materials not owned by the City including software, photographs or any other media;
E. Developing or distributing programs that are designed to infiltrate computer systems internally or externally to include development of any PC virus;
F. Accessing or downloading any resource for which there is a fee without prior department director approval;

G. Representing yourself as another user or employee.

Privacy

Employees should have no expectation of privacy while using City owned mobile devices. They are not a secure means of communication and personal or privileged information sent or received via these technologies could potentially be read or overheard by individuals other than the desired recipients. Usage records of City owned mobile devices are public record.

Violations of this policy may result in termination of access to and use of City owned mobile devices and may also result in disciplinary or legal action up to and including termination of employment, criminal or civil penalties or other legal action against the employee.

Equipment Purchase

The IT Department will meet periodically with vendors to obtain price plans, equipment and service information. A limited number of vendors will be chosen based on service offerings, price and equipment offerings. The Director of IT will facilitate any required contract negotiations for City owned mobile device service contracts.

City owned mobile phones should be reserved for times when an allowance is not conducive (such as when used on a shared vehicle or when shared as an on-call device). Requests for a City owned cell/smart phone must be approved by the department director. City owned equipment requires approval through the budget process or will require approval by the department director.

Billing

A. Mobile vendors will send monthly billing detail in either hard copy or digital format to Finance;

B. Finance will receive a consolidated invoice and is responsible for paying for the services used by the departments who have approved City owned mobile devices;

C. Any disputed charges are reported to the provider by the department that purchased the City owned mobile device. IT will not facilitate with vendors pertaining to disputes over individual mobile device use.

Personal Use

Employees whose duties require the use of a cell/smart phone may be provided one by the City upon approval by the City Manager and department director in written form. There will be no reimbursement by the City for business use of a personally owned cell phone other than through the allowance process outlined herein unless approved by the City Manager.

Cell/Smart Phone Allowance

It is the expectation of this policy that most City cell phone business will be conducted through personally owned cell/smart phones of City employees. At the discretion of the respective department director and through the budget approval process, employees may receive an allowance through payroll to cover business use of personally owned cell/smart phones. When using a personal phone subject to a phone allowance all policies in this document apply. Text messages on a personal phone are subject to open records. It is recommended to not mix City business with personal affairs in a text message as it may be subject to disclosure.

The allowance will be paid as taxable wages each pay period. Employees will obtain their own service agreements for cell/smart phones and receive an allowance from the City for the use of those services. Allowances are intended to cover cell/smart phone hardware purchases, replacement and any maintenance of devices as required. The allowance rates will be reviewed and established annually alongside the City's budget process. It is not intended that all City employees using personal cell/smart phones for business purposes will receive an allowance. Allowances will be authorized only for regular and necessary City business. Incidental and occasional use of personal cell/smart phones is expected for City business and is not to be compensated with an allowance. Those employees identified by their department directors to enroll in this program will receive the allowance as per current City policy.

A. Contracts for personally owned cell/smart phones are between the employee and the provider and are not obligations of the City. Invoices for personally owned cell/smart phone equipment or usage are not to be addressed to the City and are the employee's sole responsibility to pay;

B. Employees who receive the allowance for personally owned cell/smart phones are required to maintain current service in good standing with the cell provider so long as the allowance is in effect;

C. Employees who receive the allowance for personally owned cell/smart phones are required to make their phone numbers available for appropriate business use and to be available to answer calls on their cell/smart phones during business hours when regular business phones are not available or after normal business hours as may be appropriate or required for their position;

D. Reimbursement beyond the allowance is not provided for any reason.

XIV. Disciplinary Actions

Employees that violate any aspect of this policy may be subject to disciplinary action including revocation of certain system privileges or under appropriate circumstances disciplinary measures set forth in the employee handbook up to termination of employment.

An intern, volunteer or other quasi-employee who violates any aspect of this policy may be subject to disciplinary action including revocation of certain system privileges or under appropriate circumstances termination of their position with the City.

Violations of this policy by non-employees may be subject to revocation of system privileges and termination of business dealing with the City of Seguin.