

CITY OF SAGINAW RESOLUTION NO. 2021-06

**A RESOLUTION OF THE CITY OF SAGINAW, TEXAS, ADOPTING
INFORMATION TECHNOLOGY POLICIES AND PROCEDURES
SOCIAL MEDIA POLICIES AND PROCEDURES; AND PROVIDING AN
EFFECTIVE DATE.**

WHEREAS, the City of Saginaw, Texas, is a home rule city acting under its charter adopted by the electorate pursuant to Article XI, Section 5 of the Texas Constitution and Chapter 9 of the Local Government Code; and

WHEREAS, the City Council understands the importance of the correct usage of Information Technology; and

WHEREAS, the City Council believes that Social Media is a tool that can be utilized to provide better communication and services to the community; and

WHEREAS, the City Council desires to provide guidance to City staff using Information Technology and Social Media on the City's behalf.

**NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY
OF SAGINAW, THAT:**

1. The recitals set forth above are true and correct and are hereby incorporated into this Resolution as if set forth verbatim herein.
2. The City Council hereby approves and adopts the attached Information Technology Policies and Procedures (Attachment A) and the Social Media Policies and Procedures (Attachment B) for the City of Saginaw.

PASSED, APPROVED AND EFFECTIVE THIS ____ DAY OF _____, 2021.

APPROVED: _____
Todd Flippo, Mayor

ATTEST: _____
Janice England, City Secretary

APPROVED AS TO FORM AND LEGALITY:

Bryn Meredith, City Attorney

ATTACHMENT A

Information Technology Policies and Procedures for City of Saginaw

Objective: To establish guidelines for acceptable use of the following City Information Technology (IT) resources:

Computers, computer workstations, laptops, tablets, other end-user devices and network resources; E-mail; Internet; and Telephone and voice-mail system.

Policy

Statement: Information Technology (IT) resources owned, leased, or maintained by the City of Saginaw and data contained therein are the property of the City of Saginaw and shall be used to support legitimate City business purposes. The use of these resources imposes certain responsibilities and obligations on city officers, employees, and other authorized users and is subject to the City of Saginaw policies and applicable local, state, and federal laws.

General

Information: This policy applies to all city officers and employees and other authorized users including elected officials, board and commission members, contractors, interns, and visitors having access to the City network and other IT resources owned, leased, or managed by the City. City officers or employees and other authorized users are responsible for using these resources in a professional, lawful, and ethical manner. Although city officers or employees and other authorized users are expected to maintain the privacy and confidentiality of information to which they have access, users are not guaranteed personal privacy of any data and information, or for any activity in which they use City IT resources. All data and account audit details managed on IT resources owned, leased, or maintained by City of Saginaw may be disclosed pursuant to public information laws, and rules of discovery in the event of lawsuits or other legal actions.

Departments have the ability to define additional or enhanced Information Technology Acceptable Use policies and procedures beyond the scope of those defined in this policy. These enhancements must be documented by the Department Head and reviewed and approved by the Director of Information Technology Services (ITS) and the HR Director. The Use of City IT resources is actively monitored, and, therefore, users should have no expectation of privacy in their use of City IT resources. Identified IT resources may result in disciplinary or other appropriate action.

Policy: This policy provides a common standard for the appropriate use of City of Saginaw information technology (IT) resources to support productivity and to facilitate efficiencies in meeting daily operations and City business needs. The policy also guides prudent and responsible use in response to regulatory compliance and data security requirements.

The IT resources covered by this policy include:

All computers, computer workstations, laptops, tablets, other end-user devices, and network resources owned, leased and/or managed by City of Saginaw ITS, or connected to the city data network.

All Internet access, services and data owned, leased, managed and/or provided by City of Saginaw, and all systems and associated data supported by the City related to the management and utilization of internet access.

All **e-mail systems and services** owned, leased, managed and/or provided by City of Saginaw, including city e-mail account users, and all records and information stored at any point in time within the City's e-mail system.

All **telephone and voice-mail systems and services** owned, leased, managed or provided by City of Saginaw, and all records and information stored at any point in time within the City's telephone and voice-mail systems.

The Director of ITS, in consultation with the City Management, has the authority to revoke an individual's account access based on a determination of inappropriate use or a need to respond to known IT security issues related to any IT resources covered under this policy. Upon determination by the Director of ITS and City Management, that the identified IT issue has been mitigated, access may be subsequently restored.

Computers, Computer Workstations, Laptops, Tablets, Other End-user Devices, and Network Resources

1. Computer equipment will not be removed from premises without either prior written authorization from the Department Head or alternative established department procedures. All computer equipment when removed from City premises must be used for the purpose of conducting City business.
2. All computer equipment and peripheral storage devices that contain confidential information must be configured with encryption provided by ITS prior to removal from City premises.
3. Users shall not install or store software without prior written authorization from ITS.
4. Data not related to City business should not be stored on any City equipment or other network resource. ITS will not be responsible for personal data or other data not related to City business.
5. A user ID and password shall be required for all computers, computer workstations, laptops, tablets, and other end-user devices owned, leased or managed by City of Saginaw.
6. All computers, computer workstations, laptops, tablets, and other end-user devices, when not in use during non-working hours, must be completely shutdown. Network logoff, hibernate, and standby do not qualify as a complete shutdown.

Internet Access

1. All City officers or employees are eligible to receive internet access unless otherwise stated in writing.
2. User-level access to internet services and web sites is granted based on individual and City business requirements. ITS, in consultation with the respective Department Head, has the authority to determine and implement the appropriate level of internet access for users.
3. Temporary internet access for users who are not City officers or employees must be coordinated through ITS.

4. To ensure security standards, ITS is authorized to access, monitor, block, and capture any internet traffic or data passing through or maintained within the City IT system(s).

5. Limited personal use of the internet is permitted so long as it does not interfere with productivity, is compliant with City policy, does not interfere with any city business activity, does not compromise IT security requirements, does not consume more than an acceptable amount of IT resources (such as bandwidth), or is not listed as a prohibited.

E-mail

1. All officers and employees at City of Saginaw are eligible to receive an e-mail account, unless otherwise stated in writing.

2. When conducting City-related business via e-mail, officers or employees must use e-mail system(s) provided by the City and require a commitment by the user to transfer to the City e-mail system all e-mails that deal with City business.

3. E-mail access at City of Saginaw is controlled through individual accounts and passwords. It is the responsibility of the individual to protect the confidentiality of his or her account and password information. Each user is responsible for the content of all e-mail, including attachments sent from an individual user's account or an account for which he/she may have additional responsibility.

4. All data or information residing or originating on City e-mail systems are the sole property of the City of Saginaw and are not considered personal or private.

5. All e-mail sent or received via the city e-mail system is archived and may be subject to public access via e-discovery or public information requests. Therefore, the city e-mail system shall be used to support legitimate City business purposes only. If a user receives e-mail messages that are personal in nature, it is the responsibility of the user to communicate to the sender an alternate personal e-mail address.

6. Archival and backup copies of e-mail messages and content exist in compliance with City's records retention practices despite deletion by an individual e-mail user. Backup and archiving procedures are to ensure system and data reliability, provide for retrieval of historical e-mail account content and information, to meet regulatory requirements, and respond to potential e-discovery and other document requests.

7. E-mail that contains confidential information, protected by state or federal law shall not be transmitted without proper encryption.

8. E-mail distribution lists maintained by the ITS Department may be used only to support City business.

9. E-mail access will be removed when the individual's association with the City of Saginaw is terminated, unless other arrangements are authorized by the Director of ITS. The city is under no obligation to provide copies of, or forward any content associated with an individual's e-mail account after the user is no longer associated with the City.

10. The Director of ITS has the authority to establish best practices for e-mail account management, which may result in limitation of e-mail attachment and mailbox size.

Telephone and Voice-mail

1. Limited personal use of City telephones is allowed provided that use does not interfere with staff productivity, is compliant with City policy, does not interfere with City business activity, or consume more than an acceptable amount of resources as defined by the Department Head.

2. Personal long distance, toll-based telephone calls originating from any City telecommunication equipment is prohibited unless prior approval is obtained from the Department Head.

3. To ensure security requirements and best practice, ITS has the authority to monitor, filter, capture, and access any call data detail passing through or maintained within the City's telephone and voice-mail system(s).

Prohibited Use and Failure to Comply

Authorized users shall at all times refrain from using City IT resources for prohibited use. Prohibited use is subject to disciplinary action up to and including termination of employment or other appropriate action. Prohibited uses include but are not limited to the following illustrative list:

Conducting private or personal for-profit or unauthorized not-for-profit activities;

Conducting any solicitation for any purpose except those officially sanctioned;

Conducting any unlawful activities as defined by federal, state, or local law, regulation, or policy;

Producing, accessing, displaying, or transmitting sexually explicit, indecent, offensive, harassing or intimidating material, such as pornography or racial epithets, that could reasonably be considered threatening, offensive, intimidating, or discriminatory;

Producing, accessing, or participating in online gambling;

Attempting to modify or remove computer equipment, components, software, or peripherals without written authorization from the Department Head and Director of ITS;

Attempting to subvert the security of the City network or network resources;

Downloading, installing, or running software that reveal or create weaknesses in the security of the City network or network resources;

Accessing, copying, modifying, or deleting files, data, accounts, and access rights for applications or system functions without written authorization from the Department Head and Director of ITS;

Disclosing confidential or otherwise non-public data and information without following appropriate regulatory and/or department-specific disclosure processes;

Breaking into systems and databases or acting to disrupt the functioning of systems or causing unnecessary computing disruption.

Using City IT resources to engage in acts that unfairly monopolize IT resources for personal use to the exclusion of others. This includes streaming media (such as use of Hulu, Pandora, or Netflix) for personal use

Special Requests for Access to or Monitoring of Another User's ITS Accounts

Requests for access to or monitoring of another employee's or authorized user's ITS resources that are covered by this policy and that are owned, maintained, or leased by the City of Saginaw, such as e-mail account, voice-mail account, internet use activities, or city software systems must be submitted in writing to the Director of ITS. There are no time-based restrictions on such requests. The employee or authorized user assigned to the accounts may or may not be notified of such requests for access or monitoring or of the outcome of such requests.

Lost or Stolen Computing Equipment

Any computing equipment that is lost or stolen must be immediately reported to ITS.

E-mail

Any allegations of e-mail system(s) misuse should be promptly reported to the appropriate Supervisor, Department Head, or Director of ITS. Any user who receives an offensive e-mail, must not forward, delete, or reply to the message, but instead, report it directly to one of the individuals named above

Password Requirements - Microsoft Active Directory (network access, email, Office 365)

Passwords are an important component of information and network security. The use of a Network- ID and password combination serves to identify and authenticate a user to system resources and information assets. It is only through authenticated access that the enterprise can be assured that systems and data are being used appropriately. As such, passwords must be constructed, used and protected appropriately to ensure that the level of security they imply is met. The minimal requirements for Microsoft Active Directory passwords are as follows:

At least eight characters in length, and a maximum of 16 characters in length.

At least one upper case letter, one lower case letter, one number, and one non-alphanumeric character (!, \$, #, %).

The same password, or a like password (Example: Da!sy1234 change to Da!sy12345), cannot be reused within the previous 12 password resets.

The forced change of Active Directory passwords will occur every 90 days.

A password can only be reset once within a 24-hour period without assistance from ITS.

Passwords cannot contain a users' name (Suzy Smith) and users' account name (ssmith).

ATTACHMENT B

City of Saginaw Social Media Policies and Procedures

A. Purpose

1. The City Manager's Office has approved social networking site access in the belief that these communication tools can be utilized to provide better services to the community. The City of Saginaw encourages the use of social media to further enhance communications with various stakeholder organizations in support of The City of Saginaw goals and objectives. The City encourages the use of social media to further the goals of the City and the missions of its departments, where appropriate. This policy establishes guidelines for the use of City Social Media Sites.
2. This policy sets guidelines for use of social media to ensure timely, accurate and appropriate use of those outlets to deliver clear, concise and consistent messages on behalf of the City and to establish standards and expectations of social media use among employees and others covered by this policy.
3. This policy applies to any pre-existing or proposed social media web sites and online accounts created by City employees during the course and scope of their employment and the terms in which the public is encouraged to interact with the City in social media.
4. The following guidelines are hereby established in order to ensure professional, accurate, and timely communication with the public.

B. Scope

This policy applies to all full-time, part-time, temporary and seasonal employees as defined in City of Saginaw Employee Handbook.

C. Definitions

1. **SOCIAL MEDIA SITES** – Third party websites which allow for the creation of content and dialogue around a specific issue or area of interest (Facebook, Google+, LinkedIn, etc.).
2. **CITY SOCIAL MEDIA SITES** – Those pages, sections, or posting locations in Social Media that are established or maintained by an employee(s) of the City who is authorized to do so as part of the employee's job and that are used to conduct City business, communicate with stakeholders, or city staff, and/or communicate with or gather feedback from residents and other interested persons.
3. **CITY SOCIAL MEDIA CONTENT** – Information, images, or links posted or provided to a City Social Media Site by a City employee or authorized representative when such activity is a part of the employee's job duties.

4. SOCIAL MEDIA CONTENT -- Information, images, or links posted or provided to a Social Media Site.

5. LIMITED FORUM SITES – Clearly define a specific topic for discussion.

6. OPEN FORUM SITES – Do not limit the topic of discussion.

7. PUSH SITES – Do not allow public comments.

8. MICRO-BLOGGING SITES - Broadcast medium that exists in the form of blogging. A microblog differs from a traditional blog in that its content is typically smaller in both actual and aggregated file size. Microblogs allow users to exchange small elements of content such as short sentences, individual images, or video links. (Twitter, Tumblr, Fliptr, etc.)

9. VIDEO AND PHOTO SHARING SITES – Pages that allow users to upload their pictures to the site, which are stored on the server and made available to friends and family via personal Web pages. (Instagram, Youtube, Vimeo, etc.)

D. Policy

1. CREATION AND MAINTENANCE OF CITY SOCIAL MEDIA SITE

City Social Media Sites may contain information that represents, or may create the appearance of representing, the City's position on policy issues and/or the positions of its leadership. No employee may create or maintain a Social Media Site that purports or appears to be a City Social Media Site, except as provided herein. Before any employee or department representative may create a City Social Media Site, approval must be granted by the employee's department director, Communications Manager and City Manager. The request must state the business necessity for the City Social Media Site. For any City Social Media Sites currently in existence, the department must submit a request to continue utilizing the sites within 30 days of the effective date of this policy.

All social media accounts will be set up by the Communications Manager to ensure consistency of City brand and messaging. City social media postings by departments will be subject to approval and editing by the Communications Manager. Content may only be posted on City accounts by authorized and trained employees, in accordance with the Employee Handbook and this policy. Employees are responsible for any content they publish in any social media outlet. It is the responsibility of department directors to ensure that employees are aware of these guidelines for creating and maintaining social media resources.

Any group, department or individual representing or claiming to represent the City of Saginaw in any context of what is commonly referred to as social media or social networking on City of Saginaw-related or individual internet sites is responsible for adhering to current and future City of Saginaw policies and procedures.

Employees representing or claiming to represent the City shall not use any form of social media or social networking in any way that may blemish the City of Saginaw's integrity. Any online activity by any employee representing or claiming to represent the City that has the effect of diminishing the public's trust and/or confidence in the City of Saginaw's employees will be subject to disciplinary review. City of Saginaw employees are held to a higher standard than general members of the public and employees online activities shall reflect such professional expectations and standards.

Once a City Social Media Site is approved by the Communications Manager, the following information must be shared with the Communications Manager:

- a. All City Social Media Site login and password information (in the case of Facebook, the Communications Manager may be added as an administrator of the site instead of providing the password);
- b. Any changes to the login and password; and
- c. The names of any employees who are authorized to maintain the City Social Media Site or to post City Social Media Content ("Administrators").

The Communications Manager may disable a City Social Media Site and prohibit posting of any City Social Media Content to a site any time and for any reason, including any violation of this policy, unprofessional use of this resource, lack of use or disinterest by the public, or a department's failure to adequately maintain the site.

2. PUBLIC RECORDS

City Social Media Sites create City records that are subject to the Texas Public Information Act and document retention rules of the state of Texas. Each departmental records administrator shall ensure that such records are retained and archived in conformance with Texas law.

3. POSTING ON CITY SOCIAL MEDIA SITES

Employees creating, maintaining, or posting Social Media Content on the City Social Media Site:

- a. Must at all times conduct themselves as representatives of the City of Saginaw in accordance with all the City of Saginaw Employee Policies and Procedures and other departmental or management rules or directives;
- b. Will follow these guiding principles:
 - i. Unless the employee is posting or responding as the City Social Media Site Administrator, the employee should maintain transparency by using his/her given name and job title and clearly stating the employee's role regarding the subject;
 - ii. Use correct grammar and spelling;
 - iii. Avoid jargon;
 - iv. Write and post only about the employee's area of expertise;
 - v. Keep postings factual and accurate, do not include opinion statements;

- vi. Reply to comments in a timely manner, when a response is appropriate. When disagreeing with others' opinions or providing comments, do so in a meaningful, respectful, and relevant manner;
- vii. Understand that postings are widely accessible, not retractable, and retained or referenced for a long period of time; all content should be carefully considered;
- viii. Ensure that Social Media Content does not violate another person's privacy interests;
- ix. Refrain from posting Social Media Content that is proprietary, copyrighted (unless granted consent), attorney-client privileged, subject to state or federal privacy laws, or information not subject to disclosure under the Texas Public Information Act;
- x. Never comment on anything related to legal matters, litigation or any parties with whom the City may be in litigation without the approval of the City Attorney or the City Manager;
- xi. Never comment on anything related to HIPAA (Health Insurance Portability and Accountability Act) matters without the approval of the City Attorney or the City Manager;
- xii. Refrain from the expression of personal opinions or positions regarding:
 - (a) Programs or practices of other public agencies, political organizations, private companies, or non-profit groups;
 - (b) Political campaigns; or
 - (c) Race and religion.

Wherever possible, content posted to social media accounts will also be available on the City's website.

Wherever appropriate, content posted to social media accounts will contain links directing users to the City's website for more information.

4. DESIGN AND CONTENT OF CITY SOCIAL MEDIA SITES

Membership by the public in a City Social Media Site should not be required in order for the public to post on the site. If this is not possible on a particular City Social Media Site, then a City e-mail contact must be posted as an alternative for posting comments.

- a. The following should be clearly posted on any City Social Media Site:
 - i. A clear statement of the intent, purpose, and subject matter of the site;
 - ii. City contact information; and
 - iii. The link to the City of Saginaw website.
- b. In addition, City Social Media Sites that permit interactivity with the public, comments, or postings should post clear statements of the following in the About/BIO section:
 - i. All content and postings are subject to public disclosure;
 - ii. Users must comply with the Terms of Use of the social media site;
 - iii. Users who post or comment are legally responsible for their comments and/or posts. Comments and/or posts must not breach any law, confidentiality or copyright.
 - iv. Disclaimer that postings do not necessarily reflect the views or position of the City;
 - v. The site is not monitored 24 hours a day and that in case of an emergency the public should call 911;

- vi. All pages must contain a City of Saginaw logo and contact for the City offices including address, phone and email contacts.
 - vii. Departmental pages must clearly identify the department as a unit of the City of Saginaw.
 - viii. A link to the City's website must be present on each page.
 - ix. All pages must contain the contact information for the department office including address, phone and email contact.
- c. Each individual authorized to coordinate and post the division or department's information shall adhere to the following guidelines:
- i. Information posted should be current, accurate, complete and relevant. If mistakes are made, the site administrator must be upfront and quick with a correction.
 - ii. City pages may show links to favorite sites which are specifically related to other City departments and functions. Outside entities will not be included unless appropriate to the theme of the page. Any posted outside hyperlinks shall be accompanied by a disclaimer stating that the City of Saginaw guarantees neither the authenticity, accuracy, appropriateness nor security of the link or web site nor content linked thereto.
 - iii. Applications should not be used unless they add value to the page and support the purpose for the page. Applications that can cause security risks may be removed if it's determined that a breach may occur.
 - iv. Timeliness of postings – ensure information is posted in a timely manner. When relevant the information should be contemporaneously made available for posting to social media sites, City website, and other approved media outlets.
 - v. Be accurate – ensure facts are correct before posting to the site. Review content for grammatical and spelling errors. Employees should not post information which is inaccurate or deceptive.
 - vi. Identification – employees posting to social media sites on behalf of the City of Saginaw must identify themselves and position and take responsibility for the content they publish.
 - vii. Respect copyrights and fair use – when posting attribute information to its source
 - viii. All sites and postings shall adhere to applicable state, federal and local laws, regulations, and policies including all Information Technology and Personnel Policies.
 - ix. Professionalism – posts on social media sites should remain professional in tone and be in good taste.
 - x. If photographs are being posted, ensure the appropriate releases have been signed when needed. All pictures of individual(s) taken in non-public locations, or locations in which there may be an expectation of privacy, must have a photograph release signed or if under eighteen (18) years old signed by a parent or legal guardian before posting to any site. Written consent must be obtained to post photos taken by individuals not employed by the City.
 - xi. Sites should be restricted to informational postings only.
 - xii. The City of Saginaw reserves the right to restrict or remove any content that is deemed in violation of this policy or any applicable law.

5. EMPLOYEE TIME SPENT MAINTAINING OR CREATING CITY SOCIAL MEDIA SITES

Non-exempt employees who serve as City Social Media Site Administrators shall work on the City Social Media Site (monitoring, creating, maintaining, or posting) only during normal office hours unless specifically pre-approved in writing by the employee's supervisor. Any authorized time spent in excess of a 40-hour work week by a City Social Media Site Administrator monitoring, creating, maintaining or posting on a City Social Media Site will be paid in compliance with federal law and City policy. All time must be approved beforehand by supervisors.

E. Responsibilities

1. Department Heads are responsible for:
 - a. Ensuring that employees are aware of this policy for creating and maintaining City Social Media Sites;
 - b. Deciding who is authorized to serve as a City Social Media Site Administrator and designating appropriate access levels;
 - c. Ensuring that content that is inappropriate or violates this Policy is not posted on the City Social Media Site established and maintained by the Department; and
 - d. Ensuring that approval is sought from the Communications Manager prior to the creation of a City Social Media Site.
2. Employees are responsible for:
 - a. Ensuring that all contributions to City Social Media Sites adhere to this policy.

F. Procedures

Procedures located in the policy section above.

G. Violations of this Policy

Employees representing the City of Saginaw via social media outlets must conduct themselves at all times in accordance with all Human Resource policies. Employees will not be discourteous or disrespectful to a customer or any member of the public while in the course and scope of city business.

Employees found to be in violation of this policy will be subject to corrective action up to and including termination.