Information Technology Use

319.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the proper use of department information technology resources, including computers, electronic devices, hardware, software and systems.

319.1.1 DEFINITIONS

Definitions related to this policy include:

Computer system - All computers (on-site and portable), electronic devices, hardware, software, and resources owned, leased, rented or licensed by the St. Francis Police Department that are provided for official use by its members. This includes all access to, and use of, Internet Service Providers (ISP) or other service providers provided by or through the Department or department funding.

Hardware - Includes, but is not limited to, computers, computer terminals, network equipment, electronic devices, telephones, including cellular and satellite, pagers, modems or any other tangible computer device generally understood to comprise hardware.

Software - Includes, but is not limited to, all computer programs, systems and applications, including shareware. This does not include files created by the individual user.

Temporary file, **permanent file** or **file** - Any electronic document, information or data residing or located, in whole or in part, on the system including, but not limited to, spreadsheets, calendar entries, appointments, tasks, notes, letters, reports, messages, photographs or videos.

319.2 RESTRICTED USE

Members shall not access computers, devices, software or systems for which they have not received prior authorization or the required training. Members shall immediately report unauthorized access or use of computers, devices, software or systems by another member to a supervisor.

Members shall not use another person's access passwords, logon information and other individual security data, protocols and procedures unless directed to do so by a supervisor.

319.2.1 SOFTWARE

Members shall not copy or duplicate any copyrighted or licensed software except for a single copy for backup purposes in accordance with the software company's copyright and license agreement.

To reduce the risk of a computer virus or malicious software, members shall not install any unlicensed or unauthorized software on any department computer. Members shall not install personal copies of any software onto any department computer.

When related to criminal investigations, software program files may be downloaded only with the approval of the information systems technology (IT) staff and with the authorization of the Chief of Police or the authorized designee.

Information Technology Use

No member shall knowingly make, acquire or use unauthorized copies of computer software that is not licensed to the Department while on department premises, computer systems or electronic devices. Such unauthorized use of software exposes the Department and involved members to severe civil and criminal penalties.

Introduction of software by members should only occur as part of the automated maintenance or update process of department- or City-approved or installed programs by the original manufacturer, producer or developer of the software.

Any other introduction of software requires prior authorization from IT staff and a full scan for malicious attachments.

319.2.2 HARDWARE

Access to technology resources provided by or through the Department shall be strictly limited to department-related activities. Data stored on or available through department computer systems shall only be accessed by authorized members who are engaged in an active investigation or assisting in an active investigation, or who otherwise have a legitimate law enforcement or department-related purpose to access such data. Any exceptions to this policy must be approved by a supervisor.

319.2.3 INTERNET USE

Internet access provided by or through the Department shall be strictly limited to departmentrelated activities. Internet sites containing information that is not appropriate or applicable to department use and which shall not be intentionally accessed include, but are not limited to, adult forums, pornography, gambling, chat rooms and similar or related Internet sites. Certain exceptions may be permitted with the express approval of a supervisor as a function of a member’s assignment.

Downloaded information shall be limited to messages, mail and data files.

319.2.4 OFF-DUTY USE

Members shall only use technology resources provided by the Department while on-duty or in conjunction with specific on-call assignments unless specifically authorized by a supervisor. This includes the use of telephones, cell phones, texting, email or any other "off the clock" work-related activities.

Refer to the Personal Communication Devices Policy for guidelines regarding off-duty use of personally owned technology.

319.2 PROTECTION OF AGENCY SYSTEMS AND FILES

All members have a duty to protect the computer system and related systems and devices from physical and environmental damage and are responsible for the correct use, operation, care and maintenance of the computer system.

Members shall ensure department computers and access terminals are not viewable by persons who are not authorized users. Computers and terminals should be secured, users logged

off and password protections enabled whenever the user is not present. Access passwords, logon information and other individual security data, protocols and procedures are confidential information and are not to be shared. Password length, format, structure and content shall meet the prescribed standards required by the computer system or as directed by IT staff or a supervisor and shall be changed at intervals as directed by IT staff or a supervisor.

It is prohibited for a member to allow an unauthorized user to access the computer system at any time or for any reason. Members shall promptly report any unauthorized access to the computer system or suspected intrusion from outside sources (including the Internet) to a supervisor.

319.2 PRIVACY EXPECTATION

Members forfeit any expectation of privacy with regard to emails, texts or anything published, shared, transmitted or maintained through file-sharing software or any Internet site that is accessed, transmitted, received or reviewed on any department computer system.

The Department reserves the right to access, audit and disclose, for whatever reason, any message, including attachments, and any information accessed, transmitted, received or reviewed over any technology that is issued or maintained by the Department, including the department email system, computer network and/or any information placed into storage on any department system or device. This includes records of all keystrokes or Web-browsing history made at any department computer or over any department network. The fact that access to a database, service or website requires a username or password will not create an expectation of privacy if it is accessed through department computers, electronic devices or networks.

319.2 POLICY

It is the policy of the St. Francis Police Department that members shall use information technology resources, including computers, software and systems, that are issued or maintained by the Department in a professional manner and in accordance with this policy.

319.2 INSPECTION OR REVIEW

A supervisor or the authorized designee has the express authority to inspect or review the computer system, all temporary or permanent files, related electronic systems or devices, and any contents thereof, whether such inspection or review is in the ordinary course of his/her supervisory duties or based on cause.

Reasons for inspection or review may include, but are not limited to, computer system malfunctions, problems or general computer system failure, a lawsuit against the Department involving one of its members or a member’s duties, an alleged or suspected violation of any department policy, a request for disclosure of data, or a need to perform or provide a service.

The IT staff may extract, download or otherwise obtain any and all temporary or permanent files residing or located in or on the department computer system when requested by a supervisor or during the course of regular duties that require such information.

Former Computer Usage Replaced by Lexipol Policy 319, Information Technology Use

TITLE: COMPUTER USAGE	NUMBER: 314
EFFECTIVE DATE: 01/01/2020	REVIEW DATE: 01/01/2023

314.01 PURPOSE

The purpose of this policy is to establish guidelines for the use of the City computer system.

Definitions:

Internet: The Internet, a global information infrastructure, is a network of networks used by educators, businesses, the government, the military, and organization.

Electronic Mail: Also known as “e-mail”.

Internet Connection: The connections to the internet via metro-inet.us.

Network Supervisor: Person(s) that handles day to day functions of the network server.

Login Name: Personal code used to gain access to network services.

MIS: Management Information Systems, or data processing.

Network: This includes any references containing the word “network” such as “local area network (LAN)” and “network drives.” It refers to the computer used as the network file server, all components used in conjunction with that server, and all components used to connect computers, such as hubs, wiring, interface cards, etc.

Password: Confidential code used to gain access to network services.

314.02 POLICIES

A. Software and Hardware

1. Copyright Infringement

a. Employees are prohibited from making unauthorized copies of any copyrighted software that is owned or leased by the City of St. Francis. The City Administrator, along with the Network Supervisor, must approve the copying of any software from one computer to another. Failure to abide by federal copyright laws will expose the City of St. Francis, and the employee involved, to criminal and civil liability.

b. This applies equally to the act of bringing software from a home computer, or any other location, to be used on City of St. Francis computers. All software loaded onto City computers, including software for both network and local disk drives (c:), must be pre-approved by the Network Supervisor, or the City Administrator. To prove legal ownership of software, the original diskettes and manuals must be stored on City property.

c. The Network Supervisor will periodically check for software that may be in violation of this policy.

2. Development

a. All software programs developed for use by the City of St. Francis become property of the City. These software programs may not be sold or distributed in any manner without the written consent of proper City authorities. This includes, but is not limited to:

- All applications built using a database management system.
- All spreadsheets using Excel.
- Macros or templates created in Microsoft Word or any other word processor.
- All presentation graphics created in PowerPoint.

b. This policy may not apply to custom software developed by a third-party vendor, in which case a written contract would expressly spell out ownership rights.

B. Use of Computer Games

Computer games are not allowed on City computers. City of St. Francis employees are prohibited from using any computer game on City computers. The games that are installed as part of Windows will be removed.

C. Internet Access

1. Internet E-Mail

a. All City of St. Francis employees have a city e-mail address. During working hours, city e-mail must be used exclusively for City business.

b. Employees may write, send and read personal e-mail correspondence only on their own time.

2. Internet

Access to the Internet will be provided on all City computers. All Internet use may be monitored by the City. During working hours, Internet use will be exclusively for City business. Personal use of the Internet connection after hours is possible only with approval by the Department Head. Usenet or “Chat-

group" connections are prohibited at all times on City computers.

3. Acceptable and Unacceptable Uses of the Internet

   A. The acceptable uses of the Internet and electronic mail include the following, but are not limited to:

      a. Communication and information exchange directly related to the mission, charter, or work tasks of the City of St. Francis.

      b. Communications and exchange for professional development, to maintain currency of training or education, or to discuss issues related to the users of City activities.

      c. Use in applying for or administering grants or contracts for the City's research or programs.

      d. Use for advisory, standards, research, analysis, and professional society activities related to the user's work tasks and duties.

      e. Announcement of new City regulations, ordinances, procedures, policies, rules, services, programs, information, or activities.

      f. Any other governmental administrative communications not requiring a high level of security.

      g. Communications incidental to otherwise acceptable use, except for illegal or specifically unacceptable uses.

   B. Unacceptable uses of the Internet and electronic mail include, but are not limited to:

      a. Purposes, which violate a federal, state or local law.
      b. Any for-profit activities unless specific to the charter, mission, or duties of the City.

c. Purposes not directly related to the mission, charter, or work tasks of the City agency during normal business hours.

d. Private businesses, including commercial advertising.

e. Access to and distribution of patently offensive representations or descriptions of sexual acts.

f. Information, copies of, or modified files and other data, which are confidential under federal, state, or local law, unless specifically authorized to do so once the legal conditions for release, are satisfied.

g. Access to and distribution of material advocating intolerance of other people, races, or religions.

h. Access to and distribution of computer games that have no bearing on the City's mission. Some games that help teach, illustrate, training, or simulate agency-related issues may be acceptable.

i. Internet services or activities that interfere with or disrupt network users, services, or equipment.

j. Users intentionally representing themselves electronically as others.

k. Use for fundraising or public relations activities not specifically related to City activities.

l. Use for political activities. This includes computer equipment and resources.

C. Electronic Mail

All users of electronic mail should password protect their accounts and keep this password confidential. E-mail correspondence is considered private to the extent that under normal circumstances, it is accessible only to the user. However, e-mail messages sent or received in conjunction with government business may be releasable under the Freedom of

Information Law. In some cases, it may be accessed by the Network Supervisor.

D. Personal use

Personal use of City computer hardware and software must take place only during non-work hours and only when approved by the Department Head and the City Administrator. Work related use must not be preempted by personal use. Employees must provide their own diskettes and other supplies. Personal files may not be stored on the file server. Personal use for business, other for-profit ventures, political activities or other uses deemed by the City Administrator to be inconsistent with the City's mission is not allowed.

E. Remote Network Access

Remote access to the City of St. Francis network via modem will be allowed to certain users as authorized by the City Administrator. Access to network resources will be controlled by user login and passwords. Time limitations may be enforced if necessary.

Report Preparation

320.1 PURPOSE AND SCOPE

Report preparation is a major part of each employee's job. The purpose of reports is to document sufficient information to refresh the employee's memory and to provide sufficient information for follow-up investigation and successful prosecution. Report writing is the subject of substantial formalized and on-the-job training.

320.1.1 REPORT PREPARATION

Employees should ensure that their reports are sufficient for their purpose and reasonably free of errors prior to submission. It is the responsibility of the assigned employee to complete and submit all reports taken during the shift before going off-duty, unless permission to hold the report has been approved by a supervisor. Generally, reports requiring prompt follow-up action on active leads, or arrest reports where the suspect remains in custody should not be held.

Employees who dictate reports shall use appropriate grammar, as content is not the responsibility of the typist. Employees who generate reports on computers are subject to all requirements of this policy.

All reports shall accurately reflect the identity of the persons involved, all pertinent information seen, heard or assimilated by any other sense and any actions taken. Employees shall not suppress, conceal or distort the facts of any reported incident nor shall any employee make a false report orally or in writing. Generally, the reporting employee's opinions should not be included in reports unless specifically identified as such.

320.2 REQUIRED REPORTING

Incident reports must be completed on all dispatched calls and self-initiated events with the exception of traffic stops that result in verbal warnings.

If an officer assists another agency that officer must complete an agency assist incident report.

An officer who assists another officer within the department may complete a supplemental report at the officer's discretion if there are specific details the officer should note about their involvement with the incident. Some examples would be if the assisting officer was involved in an arrest of a subject, transport of a subject, the search and/or seizure of property, use of force on a subject, obtaining statements.

320.2.1 INJURY OR DAMAGE BY CITY PERSONNEL

Reports shall be taken if an injury occurs that is a result of an act of a City employee. Additionally, reports shall be taken involving damage to City property or City equipment.

320.3 GENERAL POLICY OF EXPEDITIOUS REPORTING

In general, all employees and supervisors shall act with promptness and efficiency in the preparation and processing of all reports. An incomplete report, unorganized reports or reports

Copyright Lexipol, LLC 2023/11/01, All Rights Reserved.

Published with permission by St. Francis Police Department

DRAFT

St. Francis Police Department

delayed without supervisory approval are not acceptable. Reports shall be processed according to established priorities or according to special priority necessary under exceptional circumstances.

320.4 REPORT CORRECTIONS

Supervisors shall review reports for content and accuracy. If a correction is necessary, the reviewing supervisor should reject the report and state the reasons for rejection. The original report should be rejected to the reporting employee for correction as soon as practicable. It shall be the responsibility of the originating employee to ensure that any report returned for correction is processed in a timely manner.

320.5 REPORT CHANGES OR ALTERATIONS

Reports that have been approved by a supervisor and submitted to the Records for filing and distribution shall not be modified or altered except by way of a supplemental report. Reviewed reports that have not yet been submitted to the Records may be corrected or modified by the authoring employee only with the knowledge and authorization of the reviewing supervisor.

320.6 FIREARM INJURY REPORTING FROM HEALTH PROFESSIONALS

Members receiving a report from a health professional of a bullet or gunshot wound, powder burns or any other injury arising from, or caused by, the discharge of any gun, pistol or any other firearm shall thoroughly investigate the facts surrounding the incident (Minn. Stat. § 626.52, Subd. 2; Minn.
Stat. § 626.553, Subd. 1).

The Records shall ensure that the report received from the health professional is forwarded to the commissioner of the Department of Health (Minn. Stat. § 626.53, Subd. 2). If the injury resulted from a hunting incident, the Records shall ensure that the findings of the investigation are forwarded to the commissioner of the Department of Natural Resources using the form provided by the commissioner (Minn. Stat. § 626.553, Sub

Former Incidents Reports Policy replaced by Lexipol Policy 320, Report Preparation

TITLE: INCIDENT REPORTS	NUMBER: 335
EFFECTIVE DATE: 01/01/2020	REVIEW DATE: 01/01/2023

335.01 PURPOSE

To establish the guidelines for documentation through incident reports.

335.02 PROCEDURE

A. All incident reports shall be factual and accurately and fully describe the circumstances surrounding an incident and the officer's involvement.

B. Incident reports must be completed on all dispatched calls and self-initiated events with the exception of traffic stops that result in verbal warnings.

C. If an officer assists another agency that officer must complete an agency assist incident report.

D. An officer who assists another officer within the department may complete a supplemental report at the officer's discretion if there are specific details the officer should note about their involvement with the incident. Some examples would be if the assisting officer were involved in an arrest of a subject, transport of a subject, the search and/or seizure of property, use of force on a subject, obtaining statements.

E. Incident reports must be completed prior to going off duty during any given shift. If circumstances arise that don't allow the officer to complete the incident report prior to going off duty the incident report should be completed as soon as possible the following day at the approval of a supervisor.

Department Use of Social Media

336.1 PURPOSE AND SCOPE

This policy provides guidelines to ensure that any use of social media on behalf of the Department is consistent with the Department's mission. Social networking in government serves two primary functions: to communicate and deliver messages directly to citizens and to encourage citizen involvement, interaction, and feedback. Information, which is distributed via social networking, must be accurate, consistent, and timely and meet the information needs of the Department's customers. Since social media is used for social networking, this policy seeks to ensure proper use of the Department's social media sites by its representatives.

Department representatives have the responsibility to use the Department's social media resources in an efficient, effective, ethical and lawful manner pursuant to all existing City and departmental policies. This policy also provides guidelines and standards for department’s representatives regarding the use of social media for communication with residents, colleagues and all other followers.

This policy applies to any existing or proposed social media web sites sponsored, established, registered or authorized by the City of St. Francis. This policy also covers the private use of the Department's social media accounts by all Department representatives. Questions regarding the scope of this policy should be directed to the Chief of Police.

Be aware that content will not only reflect on the writer but also on the City of St. Francis as a whole, including elected officials and other city employees and agents. Make sure information is accurate and free of grammatical errors. This also includes:

- Not providing private or confidential information, including names, or using such material as part of any content added to a site.
- Not negatively commenting on community partners or their services, or using such material as part of any content added to a site.
- Not providing information related to pending decisions that would compromise negotiations.
- Be aware that all content added to a site is subject to open records/right to know laws and discovery in legal cases.
- Always keep in mind the appropriateness of content.
- Comply with any existing code of ethical behavior established by the City.

This policy does not address all aspects of social media use. Specifically, it does not address:

- Personal use of social media by department members.

- Use of social media in personnel processes.
- Use of social media as part of a criminal investigation, other than disseminating information to the public on behalf of this department.

336.1.1 DEFINITIONS

Definitions related to this policy include:

Social media - Any of a wide array of Internet-based tools, mobile-based applications, websites and functions, and platforms, other than email, that allow for the sharing and discussing of information, where users can post photos, video, comments and links to other information to create content on any imaginable topic (also referred to as "user-generated content" or "consumer generated media), such as the department website or social networking services.

Social media includes but is not limited to:

- Social networking sites such as Facebook, LinkedIn, Twitter and online dating services/mobile apps
- Blogs
- Social news sites such as Reddit and Buzzfeed
- Video and photo sharing sites such as YouTube, Instagram, SnapChat, and Flickr
- Wikis, or shared encyclopedias such as Wikipedia
- An ever emerging list of new web-based platforms generally regarded as social media or having many of the same functions as those listed above.

336.2 POLICY

The St. Francis Police Department may use social media as a method of effectively informing the public about department services, issues, investigations and other relevant events. The Department will determine, at its discretion, how its web-based social media resources will be designed, implemented and managed as part of its overall communication and information sharing strategy. Department social media sites may be modified or removed by the Chief of Police or his or her designee at any time and without notice, as described in this document.

Department members shall ensure that the use or access of social media is done in a manner that protects the constitutional rights of all.

336.3 AUTHORIZED USERS

Only members authorized by the Chief of Police or the authorized designee may utilize social media on behalf of the Department. Authorized members shall use only department-approved equipment during the normal course of duties to post and monitor department-related social media, unless they are specifically authorized to do otherwise by their supervisors.

The Chief of Police may develop specific guidelines identifying the type of content that may be posted. Any content that does not strictly conform to the guidelines should be approved by a supervisor prior to posting.

Requests to post information over department social media by members who are not authorized to post should be made through the member's chain of command.

The Chief of Police is responsible for managing Department social media websites. Department members wishing to have a new social media presence must initially submit a request to the Chief of Police or his or her designee in order to ensure social media accounts are kept to a sustainable number and policies are followed. No one may establish social media accounts or websites on behalf of the Department unless authorized in accordance with this policy.

Administration of all social media web sites must comply with applicable laws, regulations, and policies as well as proper business etiquette.

When using social media sites as a representative of the Department, employees and agents will act in a professional manner. Examples include but are not limited to:

- Adhere to all Department and City personnel and Computer use policies
- Use only appropriate language.

336.4 AUTHORIZED CONTENT

Only content that is appropriate for public release, that supports the Department mission and conforms to all Department policies regarding the release of information may be posted.

Examples of appropriate content include:

(a) Announcements.

(b) Tips and information related to crime prevention.

(c) Investigative requests for information.

(d) Requests that ask the community to engage in projects that are relevant to the department mission.

(e) Real-time safety information that is related to in-progress crimes, geographical warnings or disaster information.

(f) Traffic information.

(g) Press releases.

(h) Recruitment of personnel.

336.4.1 INCIDENT-SPECIFIC USE

In instances of active incidents where speed, accuracy and frequent updates are paramount (e.g., crime alerts, public safety information, traffic issues), the Public Information Officer or the authorized designee will be responsible for the compilation of information to be released, subject to the approval of the Chief of Police or his or her designee.

336.5 PROHIBITED CONTENT

Content that is prohibited from posting includes, but is not limited to:

(a) Content that is abusive, discriminatory, inflammatory or sexually explicit.

(b) Any information that violates individual rights, including confidentiality and/or privacy rights and those provided under state, federal or local laws.

(c) Any information that could compromise an ongoing investigation.

(d) Any information that could tend to compromise or damage the mission, function, reputation or professionalism of the St. Francis Police Department or its members.

(e) Any information that could compromise the safety and security of Department operations, members of the Department, victims, suspects or the public.

(f) Any content posted for personal use.

(g) Any content that has not been properly authorized by this policy or a supervisor.

Any member who becomes aware of content on this Department's social media site(s) that he/ she believes is unauthorized or inappropriate should promptly report such content to a supervisor.
The supervisor will ensure its removal from public view and investigate the cause of the entry.

Department social media accounts may not be used for private or personal purposes of expressing private or personal views on personal, political or policy issues or to express personal views or concerns pertaining to employment relations matters.

No social media website may be used by any Department member to disclose private or confidential information. No social media website should be used to disclose sensitive information; if there is any question as to whether information is private, confidential or sensitive, contact the Chief of Police.

Authorized members will not edit any posted comments. However, social media sites are viewed as moderated online discussion sites and not as a public forum. Where moderation of comments is an available option, comments from the public will be moderated by authorized members before posting. Where moderation prior to posting is not an option, staff will regularly monitor sites. Comments posted by members of the public will be removed if they are abusive, obscene, defamatory, in violation of the copyright, trademark right or other intellectual property right of any third party, or otherwise inappropriate or incorrect. The following are examples of content that may be removed by authorized members before or shortly after being published:

- Potentially libelous comments
- Obscene or racist comments
- Personal attacks, insults, or threatening language
- Plagiarized material
- Private, personal information published without consent
- Comments totally unrelated to the topic of the moderated online discussion
- Commercial promotions or spam
- Hyperlinks to material that is not directly related to the discussion

336.5.1 PUBLIC POSTING PROHIBITED
Department social media sites shall be designed and maintained to prevent posting of content by the public.

The Department may provide a method for members of the public to contact department members directly.

336.6 MONITORING CONTENT

The Chief of Police will appoint a supervisor to review, at least annually, the use of department social media and report back on, at a minimum, the resources being used, the effectiveness of the content, any unauthorized or inappropriate content and the resolution of any issues.

336.7 DATA OWNERSHIP AND RETENTION OF RECORDS

All social media communications or messages composed, sent, or received on city equipment in an official capacity will be subject to the Minnesota Government Data Practices Act. This law classifies certain information as available to the public upon request.

The Department retains the right to monitor employee's social media use on City equipment and will exercise its right as necessary. Users should have no expectation of privacy. Social media is not a secure means of communication.

The Administration Department Supervisor should work with the Custodian of Records to establish a method of ensuring that public records generated in the process of social media use are retained in accordance with established records retention schedules.

336.8 TRAINING

Authorized members should receive training that, at a minimum, addresses legal issues concerning the appropriate use of social media sites, as well as privacy, civil rights, dissemination and retention of information posted on department sites.

336.9 POLICY VIOLATIONS

Violations of the Policy will subject the employee to disciplinary action, up to and including discharge from employment.

Former Social Media Policy Replaced by Lexipol Policy 336, Department Use of Social Media.

TITLE: SOCIAL MEDIA-CITY POLICY	NUMBER: 315
EFFECTIVE DATE: 01/01/2020	REVIEW DATE: 01/01/2023

315.01 Purpose

Social networking in government serves two primary functions: to communicate and deliver messages directly to citizens and to encourage citizen involvement, interaction, and feedback. Information, which is distributed via social networking, must be accurate, consistent, and timely and meet the information needs of the City's customers. Since social media is used for social networking, this policy seeks to ensure proper use of the City of St. Francis's social media sites by its representatives.

The City of St. Francis wishes to establish a positive and informative social media presence. City representatives have the responsibility to use the City's social media resources in an efficient, effective, ethical and lawful manner pursuant to all existing City and departmental policies. This policy also provides guidelines and standards for city representatives regarding the use of social media for communication with residents, colleagues and all other followers.

315.02 Policy

The City of St. Francis will determine, at its discretion, how its web-based social media resources will be designed, implemented and managed as part of its overall communication and information sharing strategy. City social media sites may be modified or removed by the City at any time and without notice, as described in this document.

City of St. Francis social media accounts are considered a City asset and administrator access to these accounts must be securely administered in accordance with the City's Computer Use policy. The City reserves the right to shut down any of its social media sites or accounts for any reason without notice.

All social media web sites created and utilized during the course and scope of an employee's performance of his/her job duties will be identified as belonging to the City of St. Francis, including a link to the City's official web site.

315.03 Scope

This policy applies to any existing or proposed social media web sites sponsored, established, registered or authorized by the City of St. Francis. This policy also covers the private use of the City's social media accounts by all City representatives, including its full time and part time employees, and all public safety paid on call volunteers to the extent it affects the City. Questions regarding the scope of this policy should be directed to the City Administrator.

315.04 Definition

Social media are internet and mobile-based applications, websites and functions, other than email, for sharing and discussing information, where users can post photos, video, comments and links to other information to create content on any imaginable topic. This may be referred to as "user-generated content" or "consumer-generated media."

Social media includes, but is not limited to:

- Social networking sites such as Facebook, LinkedIn, Twitter, and online dating services/mobile apps
- Blogs
- Social news sites such as Reddit and Buzzfeed
- Video and photo sharing sites such as YouTube, Instagram, SnapChat, and Flickr
- Wikis, or shared encyclopedias such as Wikipedia
- An ever emerging list of new web-based platforms generally regarded as social media or having many of the same functions as those listed above

As used in this policy, "employees and agents" means all City full time and part time employees, as well as paid volunteers.

315.05 Rules of Use

City employees and agents with administrator access are responsible for managing social media websites. Facilities or departments wishing to have a new social media presence must initially submit a request to the City Administrator or his or her designee in order to ensure social media accounts are kept to a sustainable number and policies are followed. All approved sites will be clearly marked as the City of St. Francis site and will be linked with the official City website (www.stfrancismn.org). No one

may establish social media accounts or websites on behalf of the City unless authorized in accordance with this policy.

Administration of all social media web sites must comply with applicable laws, regulations, and policies as well as proper business etiquette.

City social media accounts accessed and utilized during the course and scope of an employee's performance of his/her job duties may not be used for private or personal purposes or for the purpose of expressing private or personal views on personal, political or policy issues or to express personal views or concerns pertaining to City employment relations matters.

No social media website may be used by the City or any City employee or agent to disclose private or confidential information. No social media web site should be used to disclose sensitive information; if there is any question as to whether information is private, confidential or sensitive, contact the City Clerk.

When using social media sites as a representative of the City, employees and agents will act in a professional manner. Examples include but are not limited to:

- Adhere to all City personnel and Computer Use policies
- Use only appropriate language

Be aware that content will not only reflect on the writer but also on the City of St. Francis as a whole, including elected officials and other city employees and agents. Make sure information is accurate and free of grammatical errors. This also includes:

- Not providing private or confidential information, including names, or using such material as part of any content added to a site.
- Not negatively commenting on community partners or their services, or using such material as part of any content added to a site.
- Not providing information related to pending decisions that would compromise negotiations.
- Be aware that all content added to a site is subject to open records/right to know laws and discovery in legal cases.
- Always keep in mind the appropriateness of content.
- Comply with any existing code of ethical behavior established by the City.

Where moderation of comments is an available option, comments from the public will be moderated by City staff, with administrative rights, before posting. Where moderation prior to posting is not an option, City staff will regularly monitor sites.

City of St. Francis's staff with administrative rights will not edit any posted comments. However, City social media sites are viewed as moderated online discussion sites and not as a public forum. Comments posted by members of the public will be removed if they are abusive, obscene, defamatory, in violation of the copyright, trademark right or other intellectual property right of any third party, or otherwise inappropriate or incorrect. The following are examples of content that may be removed by City staff before or shortly after being published:

- Potentially libelous comments
- Obscene or racist comments
- Personal attacks, insults, or threatening language
- Plagiarized material
- Private, personal information published without consent
- Comments totally unrelated to the topic of the moderated online discussion
- Commercial promotions or spam
- Hyperlinks to material that is not directly related to the discussion

A. Personal Social Media Use

The City of St. Francis respects employees and agents' rights to post and maintain personal websites, blogs and social media pages and to use and enjoy social media on their own personal devices during non-work hours. The City requires employees and agents to act in a prudent manner with regard to website and internet postings that reference the City of St. Francis, its personnel, its operation or its property. Employees and agents and others affiliated with the City may not use a city brand, logo or other city identifiers on their personal sites, nor post information that purports to be the position of the City without prior authorization.

City employees and agents are discouraged from identifying themselves as city employees when responding to or commenting on blogs with personal opinions or views. If an employee chooses to identify him or herself as a City of St. Francis employee, and posts a statement on a matter related to City business, a disclaimer similar to the following must be used:

"These are my own opinions and do not represent those of the City."

Occasional access to personal social media websites during work hours is permitted, but employees and agents must adhere to the guidelines outlined in the City's Computer Use policy and the City's Respectful Workplace policy. Employees and agents should also review the Ownership section of this policy (below).

There may be times when personal use of social media (even if it is off-duty or using the employee's own equipment) may spill over into the workplace and become the basis for employee coaching or discipline. Examples of situations where this might occur include:

- Friendships, dating or romance between co-workers
- Cyber-bullying, stalking or harassment
- Release of confidential or private data; if there are questions about what constitute confidential or private data, contact the City Clerk.
- Unlawful activities
- Misuse of city-owned social media
- Inappropriate use of the city's name, logo or the employee's position or title
- Using city-owned equipment or city-time for extensive personal social media use

Each situation will be evaluated on a case-by-case basis because the laws in this area are complex. If you have any questions about what types of activities might result in discipline, please discuss the type of usage with the applicable Department Head, and then if any questions persist, the City Administrator.

315.06 Data Ownership

All social media communications or messages composed, sent, or received on city equipment in an official capacity are the property of the City and will be subject to the Minnesota Government Data Practices Act. This law classifies certain information as available to the public upon request. The City of St. Francis also maintains the sole property rights to any image, video or audio captured while a City employee is representing the City in any capacity.

The City retains the right to monitor employee's social media use on city equipment and will exercise its right as necessary. Users should have no expectation of privacy. Social media is not a secure means of communication.

315.07 Policy Violations

Violations of the Policy will subject the employee to disciplinary action up to and including discharge from employment.