



THE CITY OF SPRINGFIELD, MASSACHUSETTS

MAYOR DOMENIC J. SARNO

HOME OF THE BASKETBALL HALL OF FAME

THE CITY OF SPRINGFIELD, MASSACHUSETTS

MAYOR DOMENIC J. SARNO

EXECUTIVE ORDER

Social Media Policy

Adopted and Effective August 18, 2017.

I, Domenic J. Sarno, by authority vested in me as Mayor of the City of Springfield, Massachusetts, do hereby order that every department in the City of Springfield shall be subject to the following social media policy:

Purpose: At the City of Springfield (“Department”), we understand that social media can be a fun and rewarding way to share your life and opinions with family, friends, co-workers, or others around the world. However, use of social media also presents certain risks and carries with it certain responsibilities. To assist you in making responsible decisions about your use of social media, we have established this policy.

We are committed to ensuring our employees’ use of social media does not violate Federal or state privacy, copyright, defamation or discrimination laws. For example, City Departments are required under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) to ensure that any protected health information (“PHI”) that we create, receive, use, or store is not improperly used or disclosed through any means, including the Internet. We are also committed to, and have a legitimate interest in, protecting our provision of services, our working relationships with other organizations, our confidential and proprietary information, and reflecting favorably on our professional status as public employees and administrators.

This policy is not intended to restrict your legal rights, such as your right to engage in responsible social media discussions about things such as wages, benefits, hours, or working conditions. Rather, this policy is designed to help avoid claims against the Department or its personnel for things like: HIPAA violations, invasion of privacy and breach of contract, defamation, unlawful discrimination, and unlawful harassment. Put simply, it helps protect you

and our Department and helps ensure our members conduct themselves in a manner consistent with the City's mission of service and core values of respect and dignity toward the public, personnel we work with and to each other.

This policy will not be applied or construed in any way that might limit or improperly interfere with any applicable legal rights of Department employees, including, but not limited to, any rights under Federal or state labor laws, federal or state constitutions, nor to restrict, change or modify the rights of union members under existing collective bargaining agreements.

Scope:

This policy applies to all Department staff including but not limited to; employees, volunteers, interns, and other Department personnel. The policy applies to activity on the Internet including, but not limited to, social media sites such as Facebook, Twitter, Flickr, YouTube, Instagram, etc., as well as other websites (such as web blogs) – basically any Internet site where you can post information and/or images and communicate electronically.

Definitions:

“Confidential or Proprietary Information” includes, but is not limited to, any information that is not publicly known: internal reports, internal Department confidential communications, patient lists, and confidential information about the health of other staff members, disciplinary actions or contract negotiations.

“Protected Health Information” is any individually identifiable information that is received, created, maintained or transmitted by the Department in any form or media (electronic, paper, or oral) and relates in any way to an individual's healthcare. Individually identifiable information is information that either identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.

“Social Media” are Internet-based sites or tools that facilitate information sharing among individuals, including, but not limited to, sites such as Facebook, Twitter, Flickr, Instagram, YouTube, and other social media such as web blogs.

“Social Networking” is any means of communicating or posting information or content of any sort on the Internet, including to your own or someone else's web log or blog, journal or diary, personal web site, social networking or affinity web site, web bulletin board or a chat room, whether or not associated or affiliated with the Department.

Procedure:

In general, staff members should think carefully before posting online, because most online social platforms are open for all to see. Despite privacy policies, staff members cannot always be sure who will view, share, or archive the information that is posted. Before posting anything, you should remember

that you are responsible for what you posted online. It is always best to carefully consider the risks and rewards with respect to each posting, and to use your best judgment and exercise personal responsibility when posting to any social media sites. If you have any doubt about what you are about to post online, it is better not to post it, since once something is placed in cyberspace, it is difficult to retract the message or image.

Each Department will apply this policy in a fair and non-discriminatory manner, consistent with all applicable laws. Keep in mind that any conduct that adversely affects your job performance, the job performance of other staff members, the public, or entities we work with (including others who work on behalf of any Department), or otherwise adversely affects the legitimate business interests of a municipal Department, may result in corrective counseling or disciplinary action up to and including termination, subject to protections under existing collective bargaining agreements.

A. What You May NOT Post On the Internet and Social Media

Posting the following types of information on the Internet is specifically prohibited under this policy and may lead to corrective counseling and discipline up to and including termination:

1. Protected Health Information. You may not post or otherwise disseminate protected health information (PHI) on the Internet or social media site in any form (text, photo, audio, or video). Information that you learn and/or collect about patients while performing duties for any municipal Department is generally going to fall under the category of PHI whenever it identifies or reasonably could be used to identify a patient. Things that identify a patient include, but are not limited to, a patient's:

- First, last or full name
- Street address, city, county, or zip code
- Date of birth
- Phone number
- Social security number
- Medical record number
- Health plan number
- Account number
- Driver's license number
- Specific Incident
- Comments regarding outcome or prognosis
- Vehicle identification number or license plate number
- Image or video where the image or video shows the patient's face or other identifying feature

In addition, any information that might reasonably identify someone who is a patient could also be PHI. For example, images or videos of a patient's body or body parts, information about specific response locations and destinations, or information about the nature of an illness, injury, or incident could be enough to identify a patient and could constitute PHI. Please refer to the definition of PHI in this policy and ask your Department's HIPAA Compliance Officer if you have any questions about what is PHI. A good question to ask in order to determine whether the information is PHI is this: *Would someone who knows the patient be able to identify the patient from the information?* If so, as a general rule you should not post it.

- 2. Confidential or Proprietary Information about a municipal Department.** You may not post confidential or proprietary information about the Department or any organization or person that the Department interacts with in conducting business. This means you should not be sharing things like undisclosed details that are not publicly known or obtainable, about our contractual arrangements or other confidential business information with other parties. Please refer to the definition of confidential or proprietary information in this policy, and you may consult with a supervisor if you have any questions about what information might fall under this definition.
- 3. Explicit or Obscene Sexual Images or Content.** You may not post lewd or obscene photographs, images, or any content (text, images or videos) of a sexually explicit nature while in any municipal Department uniform or with any City or Departmental equipment or logos in view.
- 4. Unauthorized Postings Portrayed as Being From the Department.** You may not represent that you are speaking or posting on behalf of any municipal Department without the permission of the Department Head. You should never represent yourself as a spokesperson for the Department **unless you are designated** as a spokesperson for the Department.
- 5. Content That Unlawfully Harasses, Threatens, or Discriminates Against Others.** You may not post content that violates our policies against unlawful harassment and discrimination. Carefully read these policies and ensure your postings are consistent with them. Postings that include discriminatory remarks, harassment, and threats of violence or similar unlawful conduct will not be tolerated. Examples include inappropriate sexual comments about other staff members or discriminatory comments based on age, race, sex, sexual orientation, national origin, ethnicity, disability, religion, veteran's status or other legally protected class, status, or characteristic.
- 6. Sensitive Personal Information about Others.** To reduce the risk of identity theft, Medicare and Medicaid fraud, illegal stalking, and other similar illegal conduct, you should not disclose personally identifiable information (such as contact information obtained from Department files or records), Social Security numbers, credit or debit card or financial account numbers, medical insurance or account numbers or other similar information about staff members, patients, or vendors on the Internet.

7. **Use of City of Springfield or any Department Logo and Uniforms in Images or Video.** You should not use the City of Springfield Seal or any Department logo, trademark, uniform patch or proprietary graphics in any way. For example, you should not create a social media page using the City of Springfield or any of its Department's logo as this might suggest to readers that the City is sponsoring the page. You should not post images or videos of yourself or your co-workers that identify you as City staff members or that show you in a municipal Department uniform when that image or video depicts you or your co-workers engaging in what appears to be illegal or immoral conduct (such as acts of violence or the use of illegal drugs), or violations of Department policy, even if it is being done as a joke.
8. Any social media activity should not violate any of the City's Personnel or Department's published Rules and Regulations or Standard Operating Guidelines.
9. Any conduct which under a Department rule is impermissible if expressed in any other form is impermissible if expressed through social media.

B. General Rules About Social Networking Related to the Workplace

1. **No Expectation of Privacy on Agency Devices.** You should be aware that any Internet activity performed on City-owned, operated, or controlled equipment or via City Internet (hard-wired or wireless) may be monitored at any time and without notice to ensure compliance with the law, this policy and other City computer use policies. This includes City workstations, laptops, mobile data terminals, smart phones, and other electronic devices.
2. **No Access to Illegal or Pornographic Sites.** You may not access any unlawful sites or any lewd or sexually explicit sites (such as pornography sites) through City equipment or through the City's Internet connection (hard-wired or wireless) at any time. In addition, you may not access such sites with personal equipment while on City premises or at any time through City hard-wired or wireless networks.
3. **No Social Networking during Working Time.** You should not engage in social networking activities while engaged in patient care activities, while performing work duties (including when operating City vehicles or while in a City vehicle even when not driving) or when work assignments are not completed. However, you are permitted to access the Internet on your own personal equipment when you are not on working time (rest periods and meal breaks).
4. **No Taking Videos or Images during Responses or In Areas Where PHI May be Exposed.** To avoid the potential risk of improper disclosure of PHI, as well as to avoid unsafe distractions, you should refrain from taking any images or videos of any kind while on an incident response, while treating patients or otherwise engaged in work activities unless expressly authorized to do so by

your Department Head. Remember, your main focus should be public service and the incident itself.

5. Posting on Springfield Sites. The City or any of its Departments may use various Internet and social networking tools to communicate with and engage the public and our staff members. The following procedures apply:

- Only designated personnel may post on any City of Springfield or City Department social media site at the behest of the Department head or appropriate officer. The content of said posting must be reviewed by the appropriate officer prior to posting.
- On any official sites, pages, or blogs, the City will at its discretion delete spam and comments that are off-topic or inappropriate, and will reply to emails and comments when deemed appropriate.

C. Guidelines for Posting On the Internet and Social Media

1. Make it Clear you are Speaking on Your own Behalf. If it is not obvious from the content, if you post any comments about the City or its Department on the Internet you should consider:

- Disclosing your connection with the City or any of its Departments.
- Using a personal email address (not your City or Department address) as your primary means of identification and contact.

Whenever possible, you should make it clear you are speaking for yourself and not on behalf of the City or any of its Department when posting any content related to the City or any of its Departments.

Where it is not clear or obvious from the content that the post is your own opinion or view and not that of the City or any of its Departments, you should consider using the following disclaimer:

"The views expressed on this [post; blog; website] are my own and have not been reviewed or approved by my employer."

City of Springfield Social Media Policy

2017

Employee Receipt and Acknowledgement

I acknowledge that I have received a copy of the City of Springfield Social Media Policy. I have read and I understand the policy, and agree to abide by its terms during my employment with the City of Springfield. I understand that if I have a question or need clarification on this policy that I can go to my supervisor or the Department Head at any time.

Received and Read:

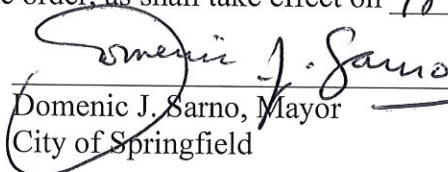
Print Name

Signature

Date

This acknowledgement will be placed in the employee's file. Failure or refusal to sign does not relieve any employee of his or her responsibility under the Policy.

This Executive order, as shall take effect on 18th of Aug., 2017.



Domenic J. Sarno, Mayor
City of Springfield