This General Order supersedes all prior rules, regulations, policies and procedures, whether oral, written or by previous practice.

POLICY STATEMENT
This policy is intended to give direction and to help Dayton Police Department employees to understand and make appropriate decisions concerning their business or personal use of social media and personal electronic device use while at work. This policy outlines the standards the department requires of all its employees when using social media, the circumstances in which the department will monitor your business or personal use of social media and the actions the department will take for a violation of this policy. This policy is not meant to address one particular form of social media; rather social media in general, as advances in technology will occur and new tools will emerge.

I. DEFINITIONS

A. Social Media: Includes all means of communicating or posting information of any sort on the internet, including but not limited to:

1. Posting to your own or someone else’s weblog or blog;
2. Posting to an internet journal or diary;
3. Posting or adding information to a personal or social media website;
4. Any activity on a social networking or affinity web site;
5. Posting or adding information to a web bulletin board/chat room or podcast; or,
6. Comments on web articles, whether or not associated or affiliated with the department, as well as any other form of electronic communication on the internet.

B. Page: The specific portion of a social media website where content is displayed. Pages are managed by an individual or individuals with administrator rights.

C. Post: Content that an individual shares on a social media site or the act of publishing content on a site.

D. Profile: Information that a user provides about an individual or an agency on a social media site.

E. Speech: Expression or communication of thoughts or opinions in spoken words; in writing; or by expressive conduct, symbolism, photographs, videotape, or related forms of communication.

F. Portable Electronic Device: An electronic device having the capability to store, record, and/or transmit text, images, videos, or audio data. Examples of such equipment include, but are not limited to, a laptop computer, cellular or wireless phone, camera, smartphone, tablet, portable digital assistant, cassette tape or digital recorder, or smartwatch.

II. BUSINESS RELATED SOCIAL MEDIA ACCOUNTS AND COMMENTS

Use of internet social media is a popular activity; however, employees must be mindful of the negative impact of inappropriate or unauthorized postings involving the Dayton Police Department and its relationship with the community.
A. Dayton Police employees who access Open Source Social Media Accounts in the performance of their official duties are required to complete Form RF-011 OSINT (Social Media) Official Duty Account User Form and forward it to the Strategic Planning Bureau Commander who will keep the information secured and on file as an investigatory work product.

Each time a social media account is opened or closed, a Form RF-011 must be completed. There are no exceptions to completing this form for any and all official accounts unless approved in writing by the Director and Chief of Police.

B. All employees authorized to post on departmental social media accounts should identify themselves and their affiliation with the department.

C. Any content posted to the department’s social media accounts should be current and accurate. If an employee does make an error in entering data on the department’s social media accounts, the employee should take responsibility for the error and immediately correct it.

D. All employees entering information on the department’s social media websites should be aware of and understand the department’s ethical code and the political activities policy to ensure compliance with the law governing such activities.

Department employees are prohibited from using or disclosing any personally identifiable information about any employee or citizen on any department social media website. If an employee finds any posting on a department social media website that includes any personally identifying information, the department employee should immediately modify or edit the posting to delete this information.

Exception: Command authorized posts involving persons of interest, including but not limited to, wanted persons, suspects in crimes, and missing individuals.

E. The department reserves the right to hide, report, or remove inappropriate employee or citizen comments on official department social media websites, whether those comments were authorized or not. Comments will be deemed inappropriate if the comments include text that:

1. Is profane, obscene or sexual;
2. Threatens or defames any person or organization;
3. Violates the legal ownership interest of another party;
4. Supports or opposes political candidates;
5. Promotes illegal activity, commercial services or products (e.g., Spam);
6. Is not topically relevant to a posting;
7. Violates federal, state, or local law, including content that is inconsistent with applicable department policies, procedures or Rules of Conduct;
8. Undermines the spirit of civil discourse intended in social media spheres.

F. If a department employee comments or adds information to a department social media account which is connected to or otherwise directly related to their employment, their comments may be monitored and are subject to moderation, including deletion/removal.

G. If a department employee adds an inappropriate comment to the department’s social media accounts, they will be disciplined, up to and including discharge.
H. Procedures

1. Speech Pursuant to Official Duties - As public employees, department personnel are cautioned that speech on- or off-duty, made pursuant to their official duties (that is, that owes its existence to the employee's professional duties and responsibilities) is not protected speech under the First Amendment and may form the basis for discipline if deemed detrimental to the department. Department personnel should assume that their speech and related activity on social media sites will reflect upon their office and this department.

2. No Expectation of Privacy - The department may monitor all business-related employee use of social media, as well as any non-business related use that occurs on department work time using department resources. The department may also monitor content posted by a department employee in furtherance of their job duties and edit, rectify, or remove any content that it deems, at its sole discretion, to violate any law, regulation, department or City policy, or that is otherwise inappropriate. Therefore, department personnel should expect that any information created, transmitted, downloaded, exchanged, or discussed in a public online forum may be accessed by the department at any time without prior notice, and should have no expectation of privacy in such content or information.

3. Applicability of other Department Policies - All other City and department policies apply in the social media context.

4. Confidentiality - Department personnel shall not post, transmit, or otherwise divulge any information that is confidential or law enforcement sensitive that is gained by reason of their employment. Employees are prohibited from disclosing or posting information or details concerning the following without the written permission from the Chief of Police or designee:
   - Criminal or traffic investigations;
   - Calls for service, traffic stops, or other contacts with citizens;
   - Crime scene images or recordings;
   - Evidence;
   - Professional Standards investigations;
   - Personnel issues, including disciplinary actions;
   - Official department training; and
   - Pending litigation.

5. Undercover Operations - Officers who work or who may reasonably be expected to work in undercover operations shall not post any form of visual or personal identification.

6. Precautions - Engaging in conduct prohibited by this policy may provide grounds for undermining or impeaching an officer's testimony in judicial proceedings.

III. SOCIAL MEDIA DURING WORK HOURS

A. An employee is not permitted to visit social media websites during work hours, unless specially authorized to do so for business-related purposes, either:
   1. due to the employee's job responsibilities; or
   2. with the express authorization of the department director.

B. Department social media accounts will be maintained and monitored by appointed department staff and personnel during regular business hours, and only those employees may access social media websites during their workday for official departmental business reasons.

C. All department staff officially tasked with entering information into the department's social media websites are responsible for adhering to this policy and ensuring that activities connected to the department's accounts on each social media platform faithfully represent the department.
D. The department will only have one account per platform unless a division or program requests permission and receives approval from the Director and Chief of Police to launch its unique account.

E. Divisions, districts and bureaus are encouraged to contact the Police Information Specialist to use the department’s centralized social media accounts to distribute public messages concerning services, operations, events, achievements, etc.

F. No employee may create or authorize an official department social media account without the prior authorization and approval of the Director and Chief of Police.

IV. USE OF PORTABLE ELECTRONIC DEVICES OR SOCIAL MEDIA WEBSITES DURING WORK HOURS

A. Department employees may not participate in social media or use portable electronic devices for non-department business while on work time, absent an emergency or prior supervisory approval. Department employees may use their portable electronic devices for personal business during their breaks or lunch period.

B. Any personal use of the department’s computers or communications equipment such as workstations, phones, laptops, or network infrastructure, to participate in social media must be minimal, occasional, limited to non-work times, and may not be at the expense of the employee’s job performance or interfere in any way with the business needs and operations of the department, and may not impose costs on the department.

C. An employee should not use their departmental email address to register on any social media website for personal use.

D. Department employees may not use their portable electronic devices or social media websites during working hours to disclose sensitive, private, or confidential department information. If there are questions about what may be considered sensitive, private or confidential, employees should check with their commander.

E. Department employees may not use a portable electronic device to videotape, record, upload, post, forward or post a picture, video, or link to any abusive, obscene, discriminatory, harassing, derogatory or defamatory content which may expose the department and the employee to legal liability.

F. Department employees may not use a portable electronic device to videotape, record, or discuss the department, your supervisors, other staff, co-workers, department issues, or department personnel issues with individuals outside of the department, in email or any other digital forum or social media, without prior individual and department approval, if said information is obtained due to their employment with the department.

G. Employees are required to get appropriate department supervisory permission before you videotape, record, refer to or post images or videos of current employees, citizens, vendors, suppliers, or department equipment or department work sites.

H. Employees are required to get appropriate permission from a former department employee before you videotape, record, refer to or post images or videos of the former employee obtained while the individual was a department employee.

V. USE OF PERSONAL SOCIAL MEDIA WEBSITES AFTER WORK HOURS

A. Whenever a department employee is using social media during their non-work hours, the department still expects that its employees will always act professionally and with dignity. Department employees should be aware that the department may observe content and information made publicly or privately available by
employees through social media. Department employees should use their best judgment in posting material that is neither inappropriate nor harmful to the department, its employees, or its citizens.

B. Department employees may not disclose sensitive, private, or confidential department information. If there are questions about what may be considered sensitive, private, or confidential, employees should check with their commander.

C. Department employees may not videotape, record, upload, post, forward, or post a picture, video, or link to any abusive, obscene, discriminatory, harassing, derogatory, or defamatory content, which may expose the department and the employee to legal liability.

D. Department employees may not videotape, record, or discuss the department, your supervisors, other staff, co-workers, department issues, or department personnel issues with individuals outside of the department, in email or any other digital forum or social media, without prior individual and department approval, if said information is obtained due to their employment with the department.

E. Employees are required to get appropriate department supervisory permission before you videotape, record, refer to or post images or videos of current employees, citizens, vendors, suppliers, or department equipment or department worksites.

F. Employees are required to get appropriate permission from a former department employee before you videotape, record, refer to or post images or videos of the former employee obtained while the individual was a department employee.

G. Impact upon the Police Department – Police Department personnel are free to express themselves as private citizens on social media sites to the degree that their speech does not impair working relationships of this department for which loyalty and confidentiality are important, impede the performance of duties, impair discipline and harmony among coworkers, or negatively affect the public perception of the department.

1. Identification as a Dayton Police Department Employee - For safety and security reasons, department personnel are discouraged from disclosing their employment with this department and are prohibited from posting information pertaining to any other member of the department without their permission. While not specifically prohibited, department personnel are discouraged from doing the following:

   a. Displaying department logos, uniforms, vehicles, or similar identifying items on personal web pages.

   b. Posting personal photographs or providing similar means of personal recognition that may cause them to be identified as a police officer of this department.

2. Rules of Conduct apply - When using social media, department personnel should be mindful that their speech becomes part of the worldwide electronic domain. Therefore, adherences to the department’s Rules of Conduct are required in the personal use of social media. In particular, department personnel are prohibited from the following:

   a. Speech containing obscene or sexually explicit language, images, or acts and statements or other forms of speech that ridicule, malign, disparage, or otherwise express bias against any race, any religion, or any protected class of individuals.

   b. Speech involving themselves or other department personnel reflecting behavior that would reasonably be considered reckless or irresponsible.
c. Speech about coworkers, supervisors or the department that is vulgar, obscene, threatening, intimidating, harassing, or a violation of the department's workplace policies against discrimination, harassment, or hostility on account of any protected class, status, or characteristic.

d. Speeches or endorsements or publish materials that could reasonably be considered to represent the views or position of the department without express authorization.

This prohibition shall not be applied to deny an employee's First Amendment rights.

3. Privacy Settings - Department personnel should be aware that privacy settings and social media sites are constantly in flux, and they should never assume that personal information posted on such sites is protected.

H. Employees of the Dayton Police Department have a right to have personal web pages or sites. When reference is made to or about the Dayton Police Department, a review of that reference is needed to ensure that such reference does not compromise our integrity and thus, undercut the public confidence in this agency or this profession.

1. While accessing and communicating on any social media site located on the Internet, regardless if it is done while conducting official, work-related business or done for personal use, employees shall conduct themselves in a manner that is consistent with the Rules of Conduct and shall not engage in any activity or present themselves in such a manner that would be detrimental to the proper functioning of the Dayton Police Department or the City of Dayton, that would impede the proper performance of work as assigned, or that would bring the professionalism of department personnel into question.

VI. LEGAL COMPLIANCE

A. This social media policy and the social media accounts of the department are intended to be legally compliant with appropriate federal, state, and local laws, regulations, and policies. Content posted on or connected to the department's social media websites is considered a public record. It is subject to the Ohio Public Records Law and other applicable record retention laws. Also, content posted by a member of the public on social media websites may be subject to e-discovery laws. Information that is protected by copyright or trademark will not be posted or maintained on a department social media account unless the owner of the intellectual property has granted permission.

VII. EMPLOYMENT REPRESENTATIONS

A. Following the end of an employee's employment with the department, the employee shall take prompt affirmative steps to ensure that no social media website or account represents you to be a current employee of the department.