

OPD – 4.1

DEPARTMENTAL GENERAL ORDER

OLIVETTE POLICE DEPARTMENT OFFICE OF THE CHIEF OF POLICE

Index as:

Department Computers

Social Networking Site

Computer Service or Repairs

COMPUTERS, TECHNOLOGY, AND SOCIAL MEDIA

I. PURPOSE

A. The purpose of this General Order is to establish guidelines to protect the integrity and security of the Department, its computers and the data created and/or stored on these computers.

B. The management and maintenance of Department computers is conducted through an Information Technologies company contracted by the City.

II. SYSTEM SECURITY:

A. Access to the Department computer network is controlled by username and password protection. Users will keep their password confidential and immediately report any breach of security to their direct supervisor.

1. The Deputy Chief, along with the City's IT contractors, will maintain the registry of the Department usernames and passwords for both in-house and REJIS computers.
2. Usernames for new employees will only be issued by the Deputy Chief. The Chief of Police will also delete usernames and passwords of employees upon the termination of their service to the Department.
3. The Deputy Chief will annually review the username and password security controls to ensure security of the system. Security lapses will be immediately brought to the attention of the Chief of Police and corrected.

B. The Department computer network is automatically backed up every day.

III. PROCEDURE

A. Use of Department computers is limited to those personnel authorized and trained to use the computers.

1. The City of Olivette owns the computers, email, and internet access systems and may monitor email and internet use for policy compliance. The City retains the right to determine what is appropriate for the workplace.

B. Email and Internet

1. Acceptable uses of the City's electronic communications systems are limited to those activities that support reference, research, internal/external communication and conducting City business in conjunction with the user's job responsibilities. The City prohibits connections to sites, or forwarding of information, that contain materials that may be offensive to others including, but not limited to, sites or information containing sexually explicit material, racially offensive material, material that makes fun of others based on political or religious beliefs, gender, sexuality or cultural practices.
2. Employees shall understand that use of any City-provided, publicly accessible computer network such as the Internet and email is a privilege. Minimal personal use of the Internet, email or other electronic communications systems is allowed under this policy as long as such use does not impede job performance or the performance of City business. The City is not responsible for personal communications sent on its electronic communications system; however, any personal use of the City's electronic communication system may be subject to the Missouri Sunshine Law and, therefore, accessible by the public.
3. Users of the City's electronic communications systems are prohibited from the following:
 - Using profanity, obscenity or other language which may be offensive or harassing to other coworkers or third parties.
 - Accessing, displaying, downloading or distributing sexually explicit material.
 - Accessing, displaying, downloading or distributing profane, obscene, harassing, offensive or unprofessional messages or content.
 - Copying or downloading commercial software in violation of copyright law.
 - Using the systems for financial gain or for any commercial activity unrelated to City business.

OPD – 4.1

- Using the systems in such a manner as to create a security breach of the City's network.
 - Looking for or applying for work or business opportunities other than for internal City postings.
 - Accessing any site, or creating or forwarding messages, with derogatory, inflammatory, or otherwise unwelcome remarks or content regarding race, religion, color, sex, national origin, age, disability, physical attributes, or sexual preferences.
 - Transmitting or sharing information regarding a coworker's health status without his or her explicit permission.
 - Expressing opinions or personal views that could be misconstrued as being those of the City.
 - Expressing opinions or personal views regarding supervisors or management of the City or other political views. Reporting unlawful conduct of supervisors or management to the appropriate party is not prohibited by this policy.
 - Using the electronic communications systems for any illegal purpose or in any way that violates City policy or is contrary to the City's best interests.
4. Except in the performance of an authorized duty, employees shall not post, transmit, reproduce, and/or disseminate information (text, pictures, video, audio, etc.) to the internet or any other forum (public or private) that would tend to discredit or reflect unfavorably upon the employee, the Department, or any of the Department's employees.
 5. Employees shall not represent themselves as an employee of this Department in a public forum with any information, opinion, or posture that would tend to discredit or reflect unfavorably upon the employee, the Department, or any of the Department's employees.
 6. Users have no expectation of privacy as the computers and all data generated by or stored on the computers is the property of the City and is subject to inspection by the Chief of Police.
 7. No software, peripherals, or additional equipment may be installed on any Department computer without the authorization of the Chief of Police.

OPD – 4.1

8. All data and records created and stored on Department computers will be considered confidential information and may only be transmitted or released outside the Department in accordance with related records policies.

C. Social Media

1. Definitions:

- a. Blog - A series of entries, written entries, written by either one person or a group of people, in an on-line journal, usually posted in chronological order, like a diary. Blogs can allow or disallow comments on entries.
- b. Comments – Responses to a blog post, news article, social media entry or other social networking post.
- c. Internet – A computer network consisting of a worldwide network of computer networks that use the TCP/IP network protocols to facilitate data transmission and exchange.
- d. Page – The specific portion of a social media website where content is displayed and managed by an individual or individuals with administrator rights.
- e. Post – The act of creating, uploading, editing or adding to any social media outlet. This includes text, photographs, audio, video or any other multimedia file.
- f. Profile – Information a user provides about him or herself on a social networking site.
- g. Social Media – On-line sources that allow people to communicate, share, and/or exchange information with others via some form of on-line or cellular network platform. Information may include, but is not limited to: text, photographs, video, audio, and other multimedia files.
- h. Social Networking – On-line platforms where users can create profiles, share information, and socialize with others using a range of technologies. This includes, but is not limited to: Facebook, MySpace, Twitter, Nixle, Flickr, YouTube, TikTok, Wikipedia, LinkedIn, Foursquare, message or on-line bulletin boards, or blogs.
- i. Speech – Expression or communication of thoughts or opinions in spoken words, in writing, by expressive conduct, symbolism, photographs, videotape, or related forms of communication.

OPD – 4.1

2. The City recognizes that many individual employees use Social Networking Sites for their own purposes. This policy does not extend to individual employee's sites, except that employees may be subject to disciplinary action for internet postings that could impair the public's confidence in the operation of City government, the Department or the performance of the individual employee.

Employees are free to express themselves as private citizens on social media sites to the degree that their speech does not negatively affect the public or professional perception of the Department.

3. Personal sites may not be designed in such a way as to cause users to believe the site is City or Department-administered or endorsed by the City or Department, including unauthorized use of City logos and trademarks. Connections with City-administered sites are permitted.
4. Employees shall abide by the following rules of conduct at all times:
 - Blogging or posting information on the Internet not relevant to City business, is not allowed during work hours.
 - Employees must never disclose any proprietary or confidential information concerning the City of Olivette or an employee of the City in a blog or other posting to the Internet, regardless if done before, during or after work hours. Posting of proprietary or confidential information may violate state law and subject the user to criminal penalty.
 - Employees must abide by all federal and state laws with regard to information sent through the Internet.
 - Employees must respect coworkers and the City. Employees must not put anything on a blog or post any information on the Internet that will defame, embarrass, insult, demean or damage the reputation of the City or any of its employees.
 - Employees must not post any pornographic pictures or other pictures of any type that could identify the posting individual as an employee of the City or any particular City of Olivette Department.
 - An employee must not post pictures of himself or herself, or others containing images of City of Olivette uniforms or insignia, City equipment or City work sites without the approval of the Chief of Police.
 - The City prohibits the unauthorized release or disclosure through the Internet or through other means of any employee information that may be considered private and/or confidential by law.

OPD – 4.1

- The City prohibits the unauthorized posting of information on the Internet that could adversely impact the City and/or an employee of the City.
5. Employees are cautioned that speech on or off-duty, made pursuant to their official duties, is not protected under the First Amendment and may form the basis for discipline if deemed detrimental to the Department.
 6. Employees' rights to express themselves as private individuals speaking on matters of public concern on social networks may not be protected under the First Amendment when such speech is outweighed by the Department's interests related to such items that:
 - interfere with the operation of the Department.
 - interfere with the maintenance of discipline by supervisors.
 - impair working relationships of the Department that are based on loyalty and confidentiality.
 - obstruct performance of duties.
 - amount to abuse of authority.
 7. Employees should assume their speech and related activity on social media sites will reflect upon their position and this Department.
 8. Employees utilizing social media, whether personally or professionally, will adhere to all Department written directives, specifically OPD-16.1 CODE OF CONDUCT.
 9. Employees are prohibited from the following:
 - a. Speech which conflicts with the Vision and Mission Statements of the Department and/or the ability of Department members to perform their duties.
 - b. Posting any of the following types of criminal justice information:
 - i. Confidential, sensitive, or copyrighted information to which they have access due to their employment with the Department.
 - ii. Data from traffic, criminal or administrative investigations including any text, photograph, audio, video, illustration, or any other multimedia file.

OPD – 4.1

- iii. Photographs of suspects, arrestees, or evidence.
 - iv. Personal statements about any investigation; including comments related to pending investigations and/or prosecutions.
10. Off-duty personnel are subject to the conditions of this Order while using Department computers.
11. Employees are subject to discipline up to and including termination for violations of this written directive.

IV. REPORTING

Any employee becoming aware of or having knowledge of a posting or of any website or web page in violation of the provisions of this policy shall notify the Chief of Police through the appropriate chain of command.

V. COMPUTER SERVICE OR REPAIRS

Problems with equipment or software will be reported promptly to the Deputy Chief through the chain of command.

This General Order supersedes all prior directives and orders inconsistent therewith.

BY ORDER OF:

Signature on File

Beth M. Andreski

Chief of Police

Effective Date: 6/30/2009

Revised: 5/18/2016

Revised: 7/16/2020

Revised: 11/3/2023

Expiration: Indefinite