POLICY & PROCEDURE

PORTAGE POLICE DEPARTMENT

SUBJECT: **COMPUTER / SOCIAL MEDIA**

SCOPE: All Department Personnel
DISTRIBUTION: Policy & Procedures Manual

REFERENCE: WI State Statute: 19.35, 995.55

NUMBER: 1.15
ISSUED: 08/22/2024
EFFECTIVE: 08/22/2024
☐ RESCINDS
☐ AMENDS
WILEAG 5TH EDITION
STANDARDS: N/A

PURPOSE: The purpose of this Policy & Procedure is to define the parameters within which Portage Police Department employees may use department property, which includes computers, internet and email services, in executing business activities; and to outline expectations of all department members with respect to their use of social media and social networking and the direct effect such use has upon the reputation and perception of the department.

This Policy & Procedure consists of the following numbered sections:

I. POLICY

A. It is the policy of the Portage Police Department that all members shall conform to established department procedures regarding computer procedures along with any restrictions of department defined social media or social networking.

II. DEFINITIONS

A. AVATAR: a computer user's representation of himself/herself, or an alter ego.

B. BLOG: a series of entries, written by either one person or a group of people, in an online journal, usually posted in chronological order, like a diary. Blogs can allow comments on entries or not.

C. BLOGGING: to read, write or edit a shared online journal. (Princeton University) Blogging can also encompass the act of commenting—and engaging with other commenters—on any blog, including one operated by a third party.

D. COMMENTS: responses to a blog post, news article, social media entry or other social networking post.

E. COMMENTING: the act of creating and posting a response to a blog post, news article, social media entry or other social networking post. Commenting can also entail the act of posting an original composition to an unrelated post or article.

F. COVERT or UNDERCOVER: an investigative activity involving the use of an assumed name or cover identity to identify criminal activity on the internet.

G. EMAIL: refers to an electronic mail system that creates stores and forwards information using telecommunication links between computer terminals, work stations, servers, or personal computers.

H. FORUM: an online discussion site.

I. HANDLE: the name of one's online identity that is used most frequently.

J. IDENTITY: an online identity, Internet identity or Internet persona that a social networking user establishes. This can be a real name, an alias, a pseudonym or a creative description.

K. INFORMATION TECHNOLOGY MANAGER: refers to the individual employee and/or Information Technology Service vendor designated by the Chief to oversee the department's Information Technology system(s).

L. 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. (Princeton University)

M. MOBILE SOCIAL NETWORKING: social networking using a mobile phone or other cellular based device.

N. POST: an item inserted to a blog or an entry to any type of computerized bulletin board or forum.

O. POSTING: the act of creating, uploading, editing or adding to any social media outlet. This includes text, photographs, audio, video or any other multimedia file

P. SOCIAL MEDIA: a variety of online sources that allows people to communicate, share information, share photos, share videos, share audio and exchange text and other multimedia files with others via some form of online or cellular network platform.

Q. SOCIAL NETWORKING: using such Internet or mobile formats to communicate with others using the same groups while also networking with other users based upon similar interests, geographical location, skills, occupation, ideology, beliefs, etc.

R. USER NAME: the name provided by the participant during the registration process associated with a Web site that will be displayed publicly on the site.

S. WORLD WIDE WEB: computer network consisting of a collection of Internet sites that offer text and graphics and sound and animation resources through the hypertext transfer protocol. (Princeton University)

III. INTERNET USAGE

A. It is the policy of the Portage Police Department to provide internet services for its employees at the department and in the squads to enhance their professional activities, improve public communication, and provide superior customer service. Efficient use of the internet for research and communication will improve the quality, productivity, and general cost effectiveness of department functions.

1. The services provided include accessing various information resources found on the internet is to enable employees to gain the level of expertise necessary to provide knowledgeable service to an increasingly sophisticated customer base.

2. The department's internet access is a privilege and the department encourages creative, professional use that enhances productivity.

B. General Guidelines

1. Internet access is provided as a business tool. When accessing the internet using department equipment and/or on department property, employees shall limit usage to appropriate job-related purposes.

2. A wide variety of information is available on the internet, some uncensored and unrestricted. The department generally does not permit access at any time to materials that may be found offensive or pornographic, except in certain official sensitive investigations.

3. Employees accessing the internet are representing the department, therefore all actions and communications shall be conducted in a manner that is consistent with the professional and courteous behavior that is expected of all department employees.

4. The transfer of information via the internet can at times be compromised. Every effort must be made to maintain a secure connection and the confidential nature of anything transmitted. The confidential nature of department information must be considered paramount.

5. Internet use and communication by employees on department equipment at all times is subject to open records and not confidential or private. The department reserves the right to monitor internet activity by employees without prior notification. Employees have no privacy with respect to their access or use of the internet.

6. Under federal and state law, and department policy, email and electronic files obtained via the internet are public records and subject at all times to inspection by the public and management in the same manner that paper documents of a similar nature are preserved and made available.

7. Many of the sites on the internet can contain computer viruses. If these viruses are downloaded, they can cause data and system corruption. Therefore, officers must be very cautious and make every effort to authenticate the origin of the file or sites before downloading or accessing.

8. No software, hardware, programs, or applications may be temporarily or permanently loaded or programming performed by any employee or other person to any department personal computer or component of the department's information system without the express knowledge and permission of the chief of police or designee.

9. The safety and security of the department's network and resources shall be considered paramount when using the internet. User passwords are confidential. It is the user's responsibility to maintain the confidentiality of their passwords.

10. All use of the internet shall be in compliance with all federal, state, and local laws and policies, including, but not limited to, those pertaining to property protection, privacy, and misuse of department resources, harassment, information security, and confidentiality. Access to the internet provided by the department shall not be used for any illegal, improper, unprofessional, or illicit purpose or for personal or financial gain.

11. In addition to the parameters outlined in this policy, employees shall use the internet in accord with the direction of the Chief of Police or designee.

C. Social Media

1. Department members are prohibited from using any department computers or cell phones/devices for any unauthorized purpose, including participation in social media or social networking for personal purposes unless authorized by the chief or designee.

2. Sworn personnel are prohibited from using any social media or social networking platform while on duty, unless permission is granted for investigative or public information purposes.

   a) A department member using social media during work time has no expectation of privacy. Members are advised that social media posts may be subject to discovery under the Freedom of Information Act and/or WI. Statute 19.35. All other litigation-related and non-litigation-related discovery devices may utilize the subject of discovery for any social media posts. Use of social media during recognized scheduled breaks away from your normal work area is allowed.

3. With discretion, officers are allowed to post general pictures which promote the department in a positive way. Further, unless granted permission by the chief of police or designee, members of this department are prohibited from posting any of the following on any social media / networking platform:

   a) Any text, photograph, audio, video, or any other multimedia file related to any investigation, both current and past, of this department.

   b) Any text, photograph, audio, video, or any other multimedia file related to any past or current action of this department, either in homage or critique.

   c) Logos, badges, seals, uniforms, vehicles, equipment or any item or symbol that is affiliated with this department.

   d) Any item, symbol, wording, number, likeness or material that is identifiable to this department.

   e) Any text, photograph, audio, video, or any other multimedia file that is related to any occurrence within the department.

4. Members who choose to maintain or participate in social media or social networking platforms while off duty shall conduct themselves with professionalism and in such a manner that will not reflect negatively upon the department or its mission. In the course of operating or participating in such venues, the following rules shall apply:

   a) Unless explicitly granted permission by the chief or designee, members shall not identify or represent themselves, in any way, as an employee of this department.

   b) Members will be held responsible for the content that appears on their maintained social media or social networking sites and will be obligated to

remove any posting or material contributed by others that identifies the member as an employee of the department.

c) Members will be held responsible for the content that appears on their maintained social media or social networking sites and will be obligated to remove any posting or material contributed by others that reflects negatively upon the department.

d) Sexually graphic or explicit material of any kind shall not be posted by the member on any form of social media or social networking site.

e) Sexually graphic or explicit material posted by others to the member's social media or social networking sites shall be immediately removed by the employee.

f) Equipment owned by this department and/or owned personally or privately, shall not be displayed or referenced to, in any multimedia format, on social media or social networking sites if such displays or depictions promote or glorify violence.

h) Any text, photograph, audio, video or any other multimedia file included on a social media or social networking site that infers, implies, states, opines or otherwise expresses the member's views on the public, legal, judicial or criminal systems shall not be detrimental to the department's mission, nor shall it in any way undermine the public's trust or confidence in this department.

i) Any posting that detracts from the department's mission will be considered a direct violation of this Policy & Procedure and subject to discipline; refer to Policy & Procedure 4.02: Disciplinary Procedures.

5. Unless serving as a permitted tool of public information or community outreach, no member shall use their rank and/or title in any social media or social networking activity, including inclusion of said rank and/or title into the member's online identity or avatar.

6. Employers who are conducting a background investigation for a potential hire, or conducting administrative or internal investigations related to performance, functionality or duties as a department employee are bound by Wisconsin State Statute 995.55 as it relates to social media. Employers may not request or require an employee or applicant for employment, as a condition of employment, to disclose access information for the personal Internet account of the employee or applicant or to otherwise grant access to or allow observation of that account. Also refer to Policy & Procedure 3.01: Recruitment and Selection and Policy & Procedure 4.03: Citizen Complaints/Internal Affairs.

7. An employee may volunteer access on their own to their private social media sites but cannot be required to do so.

8. Employers may view accounts that are open to and not restricted from public viewing.

9. Employers may request or require an employee to disclose access information to the employer in order for the employer to gain access to or operate an electronic communications device supplied or paid for in whole or in part by the employer.

D. Covert or Undercover Investigations.

The department may engage in covert internet and social networking investigations that are appropriate to carry out its law enforcement responsibilities, including the conduct of preliminary inquiries, general crime investigations, and intelligence investigations. The investigation should be well planned, deliberate and performed in compliance with all applicable policies.

The actions of undercover officers on the internet should always be appropriate, under the circumstances, and easily justified to prosecutors, judges and juries. Officers and supervisors conducting covert internet and social networking investigations will conduct such investigations under the following guidelines:

1. Officers must obtain the approval of the chief and or designee prior to the initiation of an undercover investigation involving social networking sites.

2. Social Networking investigations have no different requirements when it comes to documenting the investigations. The techniques applied on the internet still require the information be properly collected, properly preserved and properly presented in a report.

3. When possible, officers will utilize investigative computer systems and software intended to record data from the internet and audio and/or video recording in an evidentiary manner when contacting suspects.

4. Officers will not knowingly transfer or make available for download any files that contain any malicious code or other type of file that would disrupt, delay, or destroy another person's computer system.

5. The officer, or their supervisor, should notify the appropriate law enforcement agencies within the area of operation, if identified through the investigation, to ensure authentication and avoid confusion.

6. Entrapment must be scrupulously avoided.

7. Except as authorized, no undercover employee on the internet shall engage in any activity that would constitute a violation of federal, state, or local law if engaged in by a private person acting without authorization.

8. The chief or designee will only approve investigations that have a legitimate purpose and are reasonable to undertake; assure the investigator is properly prepared and trained for the assignment; determine operational

procedures, guidelines and plans; authorize undercover identities; supervise the operation; and review and approve all investigative reports and material, which are prepared and submitted by the investigating officer.

IV. EMAIL USAGE

A. General Guidelines

1. Email accounts are provided for official department business only and shall not be used for personal reasons except in the case of an emergency or specific personal business that cannot be conducted during non-working hours, and shall not be used for e-commerce, to conduct a business, or for any other personal or financial gain. Work duties shall take precedence over personal business. Employees shall conduct themselves professionally and must recognize their representation of the department and the confidentiality of department business when emailing. Email access is a privilege and shall be abused.

2. The email system maintained by the department is at all times public and subject to open records. The department provides email as a business tool. Therefore, the department reserves the right to monitor email messages without prior notification for the purpose of maintaining and supporting the department email system. Employees have no privacy with respect to their access or use of the email system.

3. The use of email for any illegal or unethical activities, which could adversely affect the department, is prohibited.

4. Various information sources can be accessed through email. Participation for business purposes is encouraged. However, approval by the Chief of Police is required before any associated costs or charges are incurred.

5. No person without specific authorization from the chief or designee shall read, alter or delete any other person’s computer files or email.

6. Under federal law, email and electronic files obtained via the Internet are public records and subject at all times to inspection by the public and management in the same manner that paper documents of a similar nature are preserved and made available.

7. The transfer of information via email can at times be compromised. Every effort must be made to maintain a secure connection and the confidential nature of anything transmitted. The confidential nature of department information must be considered paramount.

8. Email attachments can contain computer viruses. If these attachments are opened, they can cause data and system corruption. Therefore, all attachments must be checked for viruses and comply with instructions and directives from the IT Manager.

B. User Authorization

1. The department encourages email use to increase business communications and enhance one's job performance. Therefore, the Chief of Police and the IT Manager will coordinate email account access for employees.

C. Violation Of Policy

1. Violation of this policy shall be regarded as a work rule violation. Failure of an employee to adhere to and comply with these policies may result in disciplinary action up to and including discharge of employment with the city.

V. DEPARTMENT WEB SITE

A. The Chief of Police or designee may authorize certain members of the department to have access to the department's web site and only authorized members are permitted such access. In addition, the chief or designee will be in charge of all web site development, maintenance, and postings and will monitor the site content on a regular basis. All guidelines designated in III. INTERNET USAGE applies to this section.

B. The Chief of Police or designee may also determine the content allowed on the site and set guidelines specifying the content allowed or prohibited on the site. Any member who is not authorized to access the site and wants to have content posted shall contact the chief or designee for authorization.

1. Incidents that need to be posted on the web site as soon as possible (criminal investigations, missing persons, public safety issues, etc.) shall be authorized by the chief or designee, depending upon the severity of the issue and/or the need for immediate release.

C. All members that have authorization to use the site may receive training on any areas affecting the usage of the site.

D. The Chief of Police or designee shall be responsible for ensuring that any usage of the department web site is maintained according to any open records requests or retention schedules.

VI. COMPUTER HARDWARE RULES.

A. Internet use shall be governed by the policies in II.

B. Unauthorized Modifications. Once a computer system is set up and running to work efficiently with the department's software, department members shall not adjust or change any hardware switches, settings, software changes or make any other adjustments or changes without prior approval from the Chief of Police, or designee.

C. Protection of Equipment.

1. Electric charges and static electricity can destroy computer equipment, software and data. Never plug or unplug the computer or any peripheral equipment from the A.C. wall power outlet while any piece of said computer equipment is switched to the “on” position.

2. During seasons of the year when static electricity is more prevalent, always touch metal objects such as a desk (away from and not the computer desk) or other metal object to dissipate static charges before using the computer.

3. Avoid setting any liquid or food of any kind on top or next to the computer.

4. Avoid stacking books, manuals or other items against the computer when it is operating. Avoid blocking the internal cooling fan.

5. Before any cleaning of the computer is started, always make sure that the computer system and all peripherals are turned off.

D. Disposal of hardware.

1. Any computer or other device which contains a storage device (hard drive) shall have the drive removed prior to disposal.

2. Any external storage device used for official business may not be disposed of without the express consent of the Systems Administrator or designee.

3. All storage devices which are owned by the department will be made physically inoperable prior to their disposal.

4. All personally owned storage devices will be sanitized to the satisfaction of the System Administrator or designee prior to reuse or disposal.

VII. SOFTWARE POLICIES.

A. Use of department software.

1. Certain software items (computer programs) are supplied by the department for use for department related work. Do not change any setting or setup sections of any department software without prior approval from the Chief of Police or designee.

2. Never make copies of any software for any person, as unauthorized copying of copyright material such as computer software is illegal.

3. Never loan out any department software or any printed material (manuals, instruction books, reference books) accompanying department software.

4. Never erase, delete, or change any department software in any way.

5. Do not use department software for any personal business or use without prior approval from the Chief of Police or designee.

B. Non-Departmental Software.

1. Other software may be used or required to perform tasks or business for the department; however, any non-department software must be used only for police or department business and then only after approval from the Chief of Police or designee.

2. Due to malware and computer viruses only software from a secure or known source shall be submitted for approval by the Chief of Police.

Secure or known sources include: All legal commercial software, shareware or public domain software. In the case of shareware or public domain software, it will be considered to be from a secure or known source if the software comes directly from a commercial distributor or directly from the author of the software.

Insecure or unknown sources include software obtained through friends or acquaintances where the history or path of the software is unknown, and any software that has been acquired from a computer bulletin board type service.

Keith J. Klafke
Chief of Police

This Policy & Procedure cancels and supersedes any and all written directives relative to the subject matter contained herein.

Initial 08/22/2024
Updated 1-9-2026
Updated 3-23-2026