POLICY & PROCEDURE

STURGEON BAY POLICE DEPARTMENT

SUBJECT: **COMPUTER PROCEDURES**

NUMBER: 1.18

ISSUED: 12/07/2020

EFFECTIVE: 12/07/2020

SCOPE: All Department Personnel

DISTRIBUTION: Policy & Procedure Manual

☐ RESCINDS

☐ AMENDS

REFERENCE: WI State Statute: 19.35, 995.55

WILEAG 5TH EDITION

STANDARDS: N/A

INDEX AS:
Cellular Telephones
Computer Procedures
Department Property
Email Usage
Equipment, Materials or Property
Internet Usage
Laptop/Mobile Data Computer
Open Records
Public Property
Social Media

PURPOSE: The purpose of this Policy & Procedure is to define the parameters within which Sturgeon Bay 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 of such use has upon the reputation and perception of the Department.

This Policy & Procedure consists of the following numbered sections:

IV. EMAIL USAGE

V. DEPARTMENT WEB SITE

VI. COMPUTER HARDWARE RULES

VII. SOFTWARE POLICIES

I. POLICY

A. It is the policy of the Sturgeon Bay Police Department that all members shall conform to establish Department procedures regarding computer procedures along with any restrictions of Department defined social medial or social networking.

II. DEFINITIONS

A. 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.

B. INFORMATION SYSTEMS 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).

C. 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.

D. SOCIAL NETWORKING: Using such Internet or mobile formats as Facebook, Twitter, Instagram, Tik Tok, Myspace, LinkedIn, Foursquare, Gowalla Police Pulse, The Squad Room, Usenet groups, online forums, message boards or bulletin boards, blogs, and other similarly developed formats, to communicate with others using the same groups while networking with other users based upon similar interests, geographical location, skills, occupation, ideology, beliefs, etc.

E. MOBILE SOCIAL NETWORKING: Social networking using a mobile phone or other cellular based device.

F. INTERNET: A computer network consisting of a worldwide network of computer networks that use the TCP/IP network protocols to facilitate date transmission and exchange. (Princeton University)

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

H. BLOG: A series of entries, written by either on 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.

I. 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.

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

K. 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.

L. FORUM: An online discussion site.

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

N. 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.

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

P. 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.

Q. HANDLE: The name of one's online identity that is used most frequently. It can also be the name of one's Twitter identity.

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

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

III. INTERNET USAGE

A. It is the policy of the Sturgeon Bay Police Department to provide Internet services for its employees at the Department 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 World Wide Web and enabling 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 all usage to job-related purposes. The Department expects employees to conduct themselves honestly and appropriately.

2. A wide variety of information is available on the Internet, some uncensored and unrestricted. The Department does not permit access at any time to materials that may be found offensive or pornographic, nor is the Department responsible for the content of any Internet site.

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 is not secure. The confidential nature of Department information must be considered paramount. Therefore, transmittal of confidential information via the Internet is inappropriate and shall not be permitted.

5. Internet use and communication by employees on Department equipment at all times is public 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 be breeding grounds for computer viruses. If these viruses are downloaded, they can cause data and system corruption. Therefore, all downloaded files must be checked for viruses and comply with instructions and directives issued by the Information Technology Manager.

8. No software or hardware may be temporarily or permanently loaded or programming performed by any employee or other person to any Department personal computer or component of the Departments information system without the express knowledge and permission of the Information Systems Manager.

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. Employees shall abide at all times by all guidelines of this policy, and any amendments that may occur from time to time.

11. 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, sexual 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.

12. 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 his designee.

13. Department employees may not download and/or install the following types of programs:

    a) Executable Files, or Files with Extensions of .exe, .com, bat.

    b) Media Players or Real Players

    c) Software to Play Online Music, Streaming Audio, Streaming Video, or Radio Stations.

    d) Chat or Messaging Software

    e) Stock or News Tickers

f) Screen Savers

g) Social Media sites including, but not limited to: Face book, MySpace, etc.

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.
2. Sworn personnel are discouraged 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 Wisconsin 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. Unless granted explicit permission, members of this Department are prohibited from posting any of the following on social networking platforms, either on their own sites, the sites of others known to them, the sites of others unknown to them, news media pages, or other information exchange forums:

    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 Department, members are discouraged from identifying themselves, in any way, as an employee of this Department.

        NOTE: Identifying yourself as a member of this agency or law enforcement in general may bring unwanted scrutiny to your posts/accounts to include complaints, derogatory comments, harassment, etc. that may lead to internal or external investigations and possibly discipline.

    b) Members are discouraged from using any reference to infer they are employees of this Department during social media or social networking participation or maintenance.

    c) Members will be held responsible for the content that appears on their maintained social media or social networking sites.

    d) 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.

    e) 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.

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

    g) Weaponry, 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 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 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 legal, judicial or criminal systems shall not, in any way, undermine the public's trust and confidence in this Department.

j) 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 an explicitly 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 rand and/or title into the member's online identity or avatar.

6. Members who are brought under administrative or internal investigation related to their performance, functionality or duties as a Department employee may be ordered to provide the Department, or its designated investigator, with access to the social media and social networking platforms in which they participate or maintain; refer to Policy & Procedure 4.03: Citizen Complaints/Internal Affairs.

7. Department members who are brought under administrative or internal investigation related to the Department's operation, productivity, efficiency, morale, or reputation, may be ordered to provide the Department, or its designated investigator, with access to the social media and social networking platforms in which they participate or maintain.

8. If requested, any member shall complete an affidavit attesting to all the social media and social networking platforms in which they participate or maintain.

9. Due to the potential for accessing unsubstantiated, private and protected information, the Department shall not require employment candidates to provide passwords, account information or access to password-protected social media accounts.

   The Department will consider utilizing department trained personnel to conduct open source internet-based searches on candidates. However, the review of information from social media sites will ensure that:

   a) The legal rigs of the candidate are protected.
   b) Material and information to be considered are verified, accurate and validated.
   c) The department fully complies with applicable privacy protections and state and federal law.

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 crim investigations, and intelligence investigations. The investigation should be will planned, deliberate and performed in compliance with all applicable policies.

The actions of undercover officer 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. Officer must obtain the approval of the Chief 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 his/her supervisor, should notify the appropriate law enforcement agencies within the area of operation, if identified through the investigation, to ensure appropriate de-confliction has been conducted.

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 will only approve investigations that have a legitimate purpose, and are reasonable to undertake; assure the investigator is properly prepared 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.

    a) The Department expects employees to conduct themselves honestly and appropriately.

    b) Employees shall not abuse this privilege.

2. The email system is maintained by the Department on Department equipment, and at all times is public and not confidential or private. 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 support 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, or activity, which could adversely affect the Department, is prohibited.

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

5. Use of email and construction of messages must be consistent with the professional and courteous behavior that is expected of Department employees. If participating in forums, postings or list serves employees must recognize their representation of the Department, and the confidentiality of Department business.

6. No person without specific authorization shall read, alter or delete any other person’s computer files or email.

7. 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.

8. Email messages and the transfer of information are not secure. Confidential information shall not be transmitted through email and shall not be permitted.

9. Email attachments can be breeding grounds for 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 Information Systems 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 Information Systems 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 WEBSITE

A. The Chief of Police or designee may authorize certain members of the Department to have access to the Department's website, and only authorized members are permitted such access. In addition, The Chief or designee will be in charge of all website 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 have access to the site, and wants to have content posted shall contact their supervisor for authorization.

1. Incidents that need to be posted on the website as soon as possible (criminal investigations, missing persons, public safety issues, etc.) shall be authorized by the Public Information Officer 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 website 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

1. 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, margins or make any other adjustments or changes without prior approval from the Chief of Police, or whomever he/she may designate as being in charge of the computer system.

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. Never plug or unplug any cable connecting the computer or any peripheral while any part of the system is switch on.

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

4. Never set any container of liquid of any kind on top or next to the computer. One (1) drop of any kind of liquid can destroy an expensive system very quickly.

5. Always use the supplied equipment covers and cover the computer, keyboard, printer and other peripherals when you are all done. A little time spent in prevention can save many thousands of dollars.

6. Never stack books, manuals or other items against the computer when it is operating. Electric equipment produces heat, which is an enemy to safe operation of computer equipment. The computer is cooled by an internal fan, an when vents on the computer are blocked, heat will build up.

7. Before any cleaning of the computer room is started, always make sure that the computer system and all peripherals are turned off and that all equipment is covered using the supplied covers. This includes any dusting or vacuuming of any part of the room, or any other cleaning activity which may raise or produce dust.

8. Never move or jar the computer or computer desk while the computer is in operation as the hard drive is a continuously spinning device.

   Any movement could cause a “head crash” resulting in permanent damage to the hard drive and loss of data.

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. Members shall follow rules and regulations of the controlling agency when using software and other networks (i.e. Spillman, CAD, TIME System, etc.). Members shall only use such programs and software that they have authority to access.

3. Wisconsin Crime Alert Network (WICAN)- a Wisconsin Department of Justice (WIDOJ) system utilized to send crime bulletins to other law enforcement agencies and specific public recipient groups.

   a) Officers utilizing this system shall complete the WIDOJ required training prior to sending bulletins. Officers sending bulletins shall abide by WIDOJ requirements when sending bulletins.
   b) Any officer who has not been trained on the WICAN system shall request a supervisor or their designee to complete the bulletin. Officers who have been trained on the system shall receive supervisor approval before posting a bulletin.
   c) Upon receiving the requested information or ample time has passed from notification, the bulletin shall be closed on WICAN. If the suspect or relevant information is obtained, it may be shared with notifying agencies while closing the bulletin.

4. Due to the abundance of “Virus” programs that have surfaced which maliciously invade a computer system and destroy data or even equipment, 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 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.

Clinton Henry
Chief of Police

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

Initial 06/18/2020