WOONSOCKET POLICE DEPARTMENT

Thomas f. Oates, III
Chief of Police

TYPE OF ORDER	NUMBER/SERIES	ISSUE DATE	EFFECTIVE DATE
General Order	400.02	3/10/2022	3/10/2022
TITLE		**PREVIOUSLY ISSUED DATES**	
Computer, Internet and Email Usage		4/6/2015	
ACCREDITATION		**RE-EVALUATION DATE**	
CALEA Standards: 11.4.4, 41.3.7, 82.1.6 **RIPAC Standards:** 15.4		1/4/2022	
SECTION	**SUBSECTION**	**DISTRIBUTION**	
Support Operations	Communications	All Personnel	

COMPUTER, INTERNET AND EMAIL USAGE POLICY

I. PURPOSE

The purpose of this policy is to establish guidelines for the proper use of computers and other electronic equipment, systems, and/or tools under the control, ownership, or authority of the Woonsocket Police Department and/or the City of Woonsocket, R.I. These tools were provided to its employees to perform job functions including communication, exchange information and research. This policy intends to provide users with guidelines describing their responsibilities regarding confidentiality, privacy, and acceptable use of City-provided internet and email services as defined by this policy.

II. POLICY

It is the policy of the Woonsocket Police Department that the use of internet and email services provided by the city be used for legitimate police department business. Use of the internet and email services is a privilege, which imposes certain responsibilities and obligations on its users and is subject to the city ordinances, department policies, and local, state, and federal laws. Computers and other information and communication equipment are provided to employees to assist in the performance of their work.

Hardware, software, and related support systems referenced herein are defined to be the exclusive property of the Woonsocket Police Department and/or the City of Woonsocket, R.I. and the use thereof is directed towards the performance of official and proper police

duties and tasks. The user will not violate intellectual property rights, information ownership rights, or system security mechanisms.

III. DEFINITIONS

Communications: Use of electronic mail, internet, instant messaging, electronic fax, bulletin boards, television access channels, voice services, electronic subscription services including any other electronic communications forums.

Hardware: Includes, but is not limited to: tangible equipment such as computer CPUs, monitors, keyboards, printers, telephone equipment, and mobile computer components.

Software: Includes server and PC operating systems, component programs including the information stored on discs, tapes, drives, and the storage media on which said information is stored or conveyed.

Systems: Includes the components, direct or indirect, which support, facilitate, operate or compose the information and communication elements stated and to which the Woonsocket Police Department and/or the City of Woonsocket, R.I. enjoys an ownership claim or accepts a responsibility to manage and control.

Email: Electronic mail sent or received through department computer systems to include the Woonsocket City Exchange© and the Woonsocket Police records management system (RMS) email.

RILETS: Rhode Island Law Enforcement Telecommunications System

NCIC: The National Crime Information Center is a computerized index of criminal justice information (i.e. - criminal record history information, fugitives, stolen properties, missing persons). It is available to Federal, state, and local law enforcement and other criminal justice agencies and are operational 24 hours a day, 365 days a year.

CJIS: The Criminal Justice Information Services Division is a division of the United States Federal Bureau of Investigation (FBI). Programs consolidated under the CJIS Division include the National Crime Information Center (NCIC), Uniform Crime Reporting (UCR), Fingerprint Identification, Integrated Automated Fingerprint Identification System (IAFIS), NCIC 2000, and the National Incident-Based Reporting System (NIBRS).

IV. PROCEDURES

A. Communication and information systems are provided for use in the performance of official duties. These systems use are limited with the following stipulations:

1. Employees are permitted reasonable use of telephones for personal use at such times and under such circumstances that its use does not interfere with the proper performance of police work or the functioning of the phone system for police-related activities. For these reasons, employees should utilize one of the unrecorded, non-emergency lines when making a personal call.
2. Employees are not permitted to introduce, install or interface any foreign software, programming, or devices into department-owned or department-managed communications or information system components without the expressed approval of the Chief of Police or the police department's information technology (IT) services. Employees are not permitted to add, alter or delete any hardware or software component without permission as defined above.
3. All computer files, emails, and other correspondence that are produced, transmitted, or received on police department systems are the property of the police department. Police department employees' email messages sent as part of their workday are not private, but are discoverable communications and are subject to the Rhode Island Open Records Act. The police department retains the right to monitor computer use by employees, including internet browsing, emails, and other transmissions.
4. Employees are not permitted to create, transmit, download, alter, receive or distribute any information or materials which are offensive, sexually explicit, harassing, demeaning or hostile. Uses of department systems that accomplish or are intended to accomplish such purposes are considered violations of this policy.

    a. Exceptions may be made if related to a criminal investigation.

5. Computer systems are complex and vulnerable to physical and environmental abuse and neglect. Employees are responsible to exercise due care in the use of department computer equipment. Malfunctions, evidence of abuse, or violations of this regulation should be reported to a supervisor as soon as practical. Such reporting may limit system deterioration and allow for more rapid restoration.
6. Employees are expected to adhere to the instructions provided by designated department trainers in the use of information and communication system components. Such instruction includes, but is not limited to: proper methods of activating and deactivating components, performing system checks, accessing, creating, storing or sending data, employing safety checks, securing systems after use, using designated passwords and other system safeguards as directed, maintaining performance logs and related records of system operations.

V. USES OF ELECTRONIC SYSTEMS & INFORMATION

A. Electronic systems, hardware, software tools, and information are provided to conduct business for the Woonsocket Police Department. Allowable uses of electronic systems and information include the following, to the extent that these uses are to conduct business relative to the Woonsocket Police Department.

RI 15.4.a

B. To gain internet/email access, the Chief of Police must approve requests for internet access before the department's Information Technology (IT) Services will grant access. Purposes for utilization of the internet/email may be to:

1. To facilitate the performance of job functions.
2. To facilitate the communication of information promptly.
3. To communicate with departments throughout the city.
4. To communicate with outside organizations as required to perform an employee's job function.
5. All personnel is expected to read their email at least once per working day.

C. **Acceptable Use of Internet and Email activities** are those that generally do not impede the purpose, goals, and mission of the department and each user's job duties and responsibilities. The following list provides some examples of acceptable use:

1. Communications, including information exchange, for professional development or to maintain job knowledge or skills.
2. Communications with other governmental agencies providing document delivery or transferring working documents/drafts for comment.
3. Announcements of policies, procedures, laws, hearings, services, and activities.
4. Use involving research and information gathering in support of advisory, standards, analysis, and professional development activities related to the department's duties.
5. Communications and information exchanges directly relating to the mission, charter, and work tasks of the city and department including email in direct support of work-related functions or collaborative projects.
6. Communication and information exchange for investigations.

D. **Unacceptable use of Internet and Email activities**

Unacceptable use can be generally defined as activities that impede the purpose, goals, and mission of the department and the user's job duties and responsibilities. Any internet and email usage in which acceptable use is questionable should be avoided. When in doubt, seek policy clarification before pursuing the activity. Unacceptable use shall be construed as:

1. Business activities. This includes internet use for private purposes such as marketing or business transactions, private advertising of products or services.
2. Use for, or in support of, unlawful/prohibited activities as defined by federal, state, and local laws or regulations. Illegal or prohibited activities relating to internet and network access include, but are not limited to:

   a. Tampering with computer hardware or software;
   b. Knowledgeable vandalism or destruction of computer files;
   c. Transmission of threatening, obscene, or harassing materials;

d. Obscene or sexually suggestive messages or images; or
e. Solicitation for religious and political causes.

3. Using non-business software including games or entertainment software.
4. Use of the internet to try to access data that is protected and not intended for public access.
5. Violation of federal or state laws dealing with copyrighted materials or materials protected by a trade secret.
6. Intentionally seeking information about, obtaining copies of, or modifying contents of files, other data, or passwords belonging to other users, unless explicitly authorized to do so by those users.
7. Attempts to subvert network security, to impair the functionality of the network, or to bypass restrictions set by the network administrators. Assisting others in violating these rules by sharing information or passwords is also unacceptable behavior.
8. Deliberate interference or disruption of another user's work or system. Users are prohibited from performing any activity that will cause the loss or corruption of data, the abnormal use of computing resources (degradation of system/network performance), or the introduction of computer viruses by any means (use of programs with the potential of damaging or destroying programs and data).
9. Seeking exchange of information, software, etc. which is not related to one's job duties and responsibilities.
10. Use of fee-for-service providers on the internet unless the necessary approvals and funding have been obtained in advance. Any individual who obligates the city or department for services without prior approval is personally liable for these costs.
11. Use to gain access to any other internet service, which requires personnel if the user does not have proper personnel, rights, and privileges in the other service.
12. No employee shall use the internet service at any time to access sites or information that could be interpreted as demonstrating poor ethical conduct unless required as part of their official duties. These types of sites or information include, but are not limited to, those containing derogatory racial content, sexual content, derogatory religious content, offensive language, improper humor, or material that could negatively reflect on the department or city or material prohibited by law.

E. <u>Personal web pages or sites when referencing the Woonsocket Police Department.</u>

This section has been established to ensure that employees use appropriate discretion in the use of references to the **Woonsocket Police Department** and not discredit the department or employees. To further ensure inappropriate conduct is not disseminated via personal websites.

1. Employees have a right to have personal web pages or sites. When reference is made to or about the **Woonsocket Police Department** a review of that reference is needed to ensure that such reference does not cause a lack of public confidence, discredit or disrespect to the department.

2. Employees having personal web pages or other types of internet postings, which can be accessed by the public or by granted permission, shall not identify themselves directly or indirectly as an employee of the **Woonsocket Police Department** without approval as indicated in this directive.
3. Photographs or other depictions of agency uniforms, badges, patches, marked units shall not be used on employee internet postings.
4. Employees wishing to use references to or photographs/depictions noted above must receive the approval of the Chief.
5. Employees who post photos, comments, etc. of other department employees must inform and seek approval from the employee(s) before posting the same.
6. Any employee becoming aware of or know of a posting and/or website in violation of the provisions of this policy shall notify a supervisor immediately for follow-up action.
7. Sites deemed inappropriate, whether an employment association or not, bringing discredit to the department and or employees, in addition, promoting misconduct whether on or off duty may be investigated through a criminal or administrative investigation.

F. Approval Process

The employee seeking approval to use references to the agency on personal web pages or sites shall:

1. Submit a request for approval to the Chief of Police via the Chain-of-Command.
2. Describe the proposed reference to the agency and purpose.
3. Provide a list and media to be used on the web page.
4. If available provide a printed layout of the entire web page, posting, or site.
5. The employee will receive an approval or denial of the request.

G. Limitations

1. No sexual, violent, racial, ethnically derogatory material, comments, pictures, artwork, video, or other references may be posted along with any agency-approved reference.
2. Employees shall not post any material on the internet that brings discredit to or may adversely affect the efficiency or integrity of the agency.
3. Employees should consider the possible adverse consequences of internet postings, such as future employment, cross-examination in criminal cases, and public as well as private embarrassment.
4. Employees are encouraged to seek the guidance of supervisors regarding any posting that may adversely reflect upon either the agency or upon the professionalism or integrity of the employee.

H. Change Approval

Any changes made to a previously approved web page, site, or posting must be submitted for reconsideration.

VI. PASSWORDS/SECURITY

The IT Services will maintain, as a minimum, a password security level on the department's office agency computer systems, but primary computer resources security is the responsibility of the individual member.

1. Access to data on the agency computer systems will be secured using strong passwords and menu programs. The menus will contain options necessary for specific users or groups of users. Access to programs and menus will be granted on an as-needed basis only.
2. Passwords will:

    a. Be at least eight alphanumeric characters long.
    b. Include at last one number.
    c. Include at least one special character, e.g. !@#$%^&*().

3. Passwords will not be:

    a. A word within any language, slang, dialect, jargon, etc.
    b. Based on personal information, names of family, etc.
    c. Based on a song title, affirmation, or other phrases.

4. All passwords must be changed at least every ninety (90) days.
5. All department computers will have the screen lock feature enabled requiring personnel to reenter their password after thirty (30) minutes of inactivity.
6. RILETS/NCIC access will utilize the username issued by RILETS, a personal identification number (PIN), and a passcode generated from issued tokens.
7. Passwords will not be inserted in emails or other electronic communication.

RI 15.4.d

8. Personnel assigned a personal computer, laptop or tablet must make every reasonable effort to maintain the security of the hardware, software, and data.
9. Each member is responsible for all reports generated, data displayed, and data changes while signed on to agency computer systems under the member's user ID.
10. Personnel shall not divulge or share their own or another person's password with any member.
11. Personnel shall not use the "Remember Password" feature of applications.
12. Personnel will not write passwords down and store them anywhere in their assigned workspace.
13. Personnel shall not sign on to agency computer systems for the use of any other member, nor shall any member sign-on or use a device connected to agency computer

systems with another member's password, other than routine team functions approved by a supervisor.

14. No member shall make any attempt to learn the password of any other member or attempt to break established password security.
15. Any personnel knowing or having a suspicion that their password has been compromised, shall immediately request their password be changed in writing and explain the reason why the change is necessary to IT Services.
16. All non-sworn personnel and/or contractors who have access to the facilities will be required to attend Security Awareness Training to conform to RILETS/CJIS rules of behavior.

RI 15.4.e

17. The IT Manager shall ensure that an annual audit of all active user accounts and passwords to ensure that no unauthorized accounts and/or passwords remain active
18. All user accounts and passwords that are no longer needed must be deleted or disabled immediately. This includes but is not limited to:

    a. When a user retires, resigns, is released, dismissed, etc.
    b. Default passwords shall be changed immediately on all equipment.
    c. Intern/contractor accounts when no longer needed to perform their duties.

19. When user accounts and passwords are no longer needed, the following procedures should be followed:

    a. The employee should notify their immediate supervisor.
    b. Intern/contractor should notify their point-of-contact.
    c. The supervisor should notify IT services via departmental email.
    d. IT services will then delete and/or suspend the user's account and password.
    e. The Operations Captain will check to ensure the password and user account have been deleted and/or suspended.

VII. REMOTE ACCESS

A. Only authorized personnel shall be granted remote access to department networks.
B. Remote access is to be controlled by using either a Virtual Private Network (VPN) in which a password and user ID are required or a form of advanced authentication (i.e. biometrics, tokens, Public Key Infrastructure (PKI), certificates, etc.)

VIII. BACK UP FILES

RI 15.4.b
RI 15.4.c

A. Whenever an employee creates a computer-generated document that may have residual value after initial development and printing and may need to be stored and recalled from a computer database, should be backed up to protect against loss due to computer failure or system corruption. Documents meeting these criteria should be stored on the shared folder on the department file server after having been given a unique file name for storage by the user.

B. The police department IT services may inspect individual systems to ensure that adequate backup procedures are being employed to protect and retain important department data.

IX. REVOCATION OF PRIVILEGES

Access privileges to the department's information technology resources will not be denied without cause. If in the course of an investigation, it appears necessary to protect the integrity, security, or continued operation of its computers and networks or to protect itself from liability, the department may temporarily deny access to those resources. Alleged policy violations will be referred to appropriate departmental investigative and disciplinary procedures. The department may also refer any other suspected violations of law to other appropriate law enforcement agencies.

Users having access to city-provided internet and email services are advised that all such network activity is the property of the city, and therefore, they should not consider any activity to be private.

Per order,

Thomas F. Oates, III

Chief of Police

Written directives published within PowerDMS are in full force and effect on the referenced dates and have been approved by the Chief of Police