City of Ogdensburg, NY
330 Ford Street

Internet Technology
Policies Employee Handout
June 29, 2018

ARTICLE XIV
INTERNET TECHNOLOGY POLICIES

§AR- 85. PURPOSE

Every officer, City employee, Non-City employee or contractor shall be subject to and abide by the Internet Technology Policies of the Code of the City of Ogdensburg.

§AR- 86. EMAIL USE POLICY

A. Purpose and Goals

E-mail is one of the City of Ogdensburg's core internal and external communication methods. The purpose of this policy is to ensure that e-mail systems used by City staff support City business functions to their fullest capacity. This policy advises staff and management of their responsibilities and provides guidance in managing information communicated by e-mail. All City e-mail is the property of the City of Ogdensburg.

B. Access to E-mail Services

E-Mail services are provided to staff whose job functions require it and as resources allow. Access requests must be made by Department Heads for each employee to the Email Administrator.

The Department Head must notify the Email Administrator immediately when an e-mail user separates employment (retirement, resignation, etc.) with the City. The Email Administrator will be responsible for removing user credentials immediately.

C. Use of E-Mail

E-mail services, like other means of communication, are to be used to support City business. Staff may use e-mail to communicate informally with others in the City so long as the communication meets professional standards of conduct. Staff may use e-mail to communicate outside of the City when such communications are related to legitimate business activities and are within their job assignments or responsibilities. Staff will not use e-mail for illegal, disruptive, unethical or unprofessional activities, or for personal matters or for any purpose that would jeopardize the legitimate interests of the City.

D. Privacy and Access

E-mail messages are not personal or private. E-mail system administrators will not routinely monitor individual staff member's e-mail and will take reasonable precautions to protect the privacy of e-mail. However, management and City network administrators may access an employee's e-mail:

(1) for a legitimate business purpose (e.g., the need to access information when an employee is absent for an extended period of time);
(2) to diagnose and resolve technical problems involving system hardware, software, or communications;
(3) to investigate possible misuse of e-mail when a reasonable suspicion of abuse exists or in conjunction with an approved investigation; and,
(4) of will for any reason.

a. A staff member is prohibited from accessing another user's e-mail without his or her permission.

b. E-mail messages sent or received in conjunction with City business may:

(1) be releasable to the public under the Freedom of Information Law
(2) require special measures to comply with the Personal Privacy Protection Law

c. All e-mail messages including personal communications may be subject to discovery proceedings in legal actions.

E. Security

E-mail security is a joint responsibility of the Email Administrator and e-mail users. Users must take all reasonable precautions, including safeguarding passwords, to prevent the use of the account by unauthorized individuals.

F. Management and Retention of E-mail Communications

(1) Applicable to all e-mail messages and attachments

a. E-mail is a communications system and messages should not be retained for extended periods of time. Users should remove all e-mail communications in a timely fashion. If a user needs to retain information in an e-mail message for an extended period, he or she should transfer it from the e-mail system to an appropriate electronic or other filing system (e.g. Microsoft Outlook).

(2) Applicable to records communicated via e-mail

E-mail created in the normal course of official business or retained as evidence of official policies, actions, decisions or transactions are records subject to records management requirements. Examples of messages sent by e-mail that typically *are records* include:

- policies and directives
- correspondence or memoranda related to official business
- work schedules and assignments
- agendas and minutes of meetings
- drafts of documents that are circulated for comment or approval
- any document that initiates, authorizes or completes a business transaction
- final reports or recommendations

(3) Some examples of messages that *typically do not constitute records* are:

- copies or extracts of documents distributed for convenience or reference
- phone message slips

G. Record Retention

(1) Records communicated using e-mail need to be identified, managed, protected and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Records needed to support program functions should be retained, managed and accessible in an existing filing system outside the e-mail system in accordance with the appropriate program unit's standard practices.

(2) Records communicated via e-mail will be disposed of within the record keeping system in which they have been filed in accordance with a Records Disposition Authorization (RDA) approved by State Archives and Records Administration (SARA). Management should consult with the City Records Management Officer concerning RDAs applicable to their program's records.

(3) Users should:

- dispose of copies of records in e-mail after they have been filed in a record keeping system; and,
- delete records of transitory or little value that are not normally retained in record keeping systems as evidence of City activity.

H. Roles and Responsibilities

(1) City management will insure that policies are implemented by program. Management will develop and/or publicize record keeping practices in their area of responsibility including the routing, format and filing of records communicated via e-mail. They will train staff in appropriate use and be responsible for ensuring the security of physical devices, passwords and proper usage.

(2) City network administrators and e-mail users are responsible for e-mail security, backup and disaster recovery.

(3) All e-mail users shall:

- Be courteous and follow accepted standards of etiquette
- Protect others' privacy and confidentiality
- Facilitate organizational access before sending, filing or destroying e-mail messages
- Protect their passwords
- Remove transient records and reference copies in a timely manner
- Comply with City policies, procedures and standards
- Not use e-mail for personal matters

I. Policy Review and Update

(1) The Email Administrator or designee will periodically review and update this policy as new technologies and organizational changes are planned and implemented. Questions concerning this policy should be directed to your Department Head.

(2) All City employees shall sign a City of Ogdensburg Email Use Policy User Agreement.

§ AR-87. NETWORK & INTERNET ACCEPTABLE USE POLICY

A. Purpose

(1) The City of Ogdensburg's connection to the global Internet exists to facilitate the official work of the City of Ogdensburg. The Internet facilities and services will contribute broadly to the missions of the City of Ogdensburg.

(2) The Network and Internet connections and services are provided for employees and persons legitimately affiliated with the City of Ogdensburg for the efficient exchange of information and the completion of assigned responsibilities consistent with the City of Ogdensburg's statutory purposes.

a. The Department Head must notify the IT Administrator immediately when a network and internet user separates employment (retirement, resignation, etc.) with the City. The IT Administrator will be responsible for removing user credentials immediately.

B. Ogdensburg Computer Network

(1) City owned computer systems and all information contained within is the property of the City of Ogdensburg. They are provided to enable City employees to work more efficiently and effectively and are not for personal use. When it improves an employee's productivity and effectiveness, use of a PC is encouraged.

(2) Employees should not assume that any computer equipment or technologies, such as electronic mail and data are confidential or private. The City maintains the right and ability to enter these computer systems to access and review any information at any time without notice to the employees.

a. Department heads shall be responsible for ensuring that all computer users know and understand safe computing practices. This shall include, but is not limited to:

1. Performing frequent backups on data files.
2. Using anti-virus software to scan for viruses on all files that are downloaded from the Internet or any other outside source.
3. Don't click or download things that you didn't solicit. Even saying no thank you (by clicking) gives them information about you. If you click something and then suspect it was not legitimate, report it immediately to the IT Administrator.
4. Don't download "free" software. Nothing is free. Often these free applications come with spyware and other malware including viruses.
5. Instances of malfunctioning computer equipment shall be reported to the IT Administrator immediately.
6. In the event of a serious virus outbreak or in the case of a continued break of this policy by an employee, the employee will be disconnected from the Internet and the City's other computer systems until such time as he/she again complies with the City's computer policy.
7. Computer equipment (e.g. Non-City computers/equipment, USB/thumb drives, files on cd/dvd, external drives, etc.) installed, moved, changed or modified without the authorization of the Contracted IT Technician and/or the IT Administrator is

prohibited.

8. Any unauthorized equipment or software not supported by the City that creates or causes technical problems or malfunctions of the City technology infrastructure shall be immediately removed by the Contracted IT Technician and/or the IT Administrator.

b. The use of the Internet facilities by any employee or other person authorized by the department must be consistent with the Acceptable Use Policy and security policies.

C. **Principles of Acceptable Use**

(1) City of Ogdensburg Internet users are required:

- To respect the privacy of other users; for example, users shall not intentionally seek information on, obtain copies of or modify files or data belonging to other users unless explicit permission to do so has been obtained.
- To respect the legal protection provided to programs and data by copyright and license.
- To protect data from unauthorized use or disclosure as required by State and Federal laws and City of Ogdensburg regulations and policies.
- To respect the integrity of computing systems; for example, users shall not use or develop programs that harass other users or infiltrate a computer or computing system and/or damage or alter the software components of a computer or computing system.
- To safeguard their accounts and passwords. Any user changes of passwords must follow City of Ogdensburg guidelines for good passwords. Accounts and passwords are assigned to single users and are not to be shared with any other person without authorization. Users are expected to report any observations of attempted security violations.

D. Unacceptable Use:

(1) It is not acceptable to use City of Ogdensburg Internet facilities:

- For activities unrelated to the City of Ogdensburg's mission
- For activities unrelated to office assignments and/or job responsibilities
- For any illegal purpose
- To transmit threatening, obscene or harassing materials or correspondence
- For unauthorized distribution of City of Ogdensburg data and information
- To interfere with or disrupt network users, services or equipment
- For private purposes such as marketing or business transactions
- For solicitation for religious and political causes
- For unauthorized not-for-profit business activities
- For private advertising of products or services

- For any activity meant to foster personal gain
- For personal use

(2) The City of Ogdensburg reserves the right to remove a user account from the network.

E. Web 2.0 and Social Networking

(1) Social networking (e.g. Facebook, Twitter, etc.) and other Web 2.0 technologies (blogs, wikis, Youtube, etc.) can help drive the City's mission and support professional development. However, improper uses of Web 2.0 technologies raise a number of security and reputational risks and the potential for widespread damage to the government entity. If use of Web 2.0 and other social networking technologies is permitted by the user's supervisor, users must adhere to the following guidelines when using such technologies on City IT resources:

- All policies and work rules apply when participating in a social network or using a Web 2.0 technology for business use. Users are responsible for all of their on line activities that are: conducted with a City e-mail address; can be traced to the City's domain; and/or use City resources.
- Users must not discuss or post confidential information.
- Users should be transparent when participating in any online community by disclosing their identity and affiliation with the City.
- Users should communicate in a professional manner
    - Be direct, informative and brief
    - Fact-check posts and include links to source information
    - If possible, spell and grammar check everything and correct errors promptly
- Abide by copyright and other applicable laws. Participation online results in a user's comments being permanently available and open to being republished in other media. Users should be aware that libel, defamation, copyright and data protection laws apply.
- Ensure that the terms of service for social networking sites comply with State laws.
- When communicating on behalf of the City, obtain necessary authorizations from their supervisor.
- Obtain permission before publishing photographs, videos or quotes of others.

(2) The City of Ogdensburg will not be responsible for any damages. This includes the loss of data resulting from delays, non-deliveries or service interruptions caused by negligence, errors or omissions. Use of any information obtained is at the user's risk. Any computer connected to a network should have anti-virus software installed. The City of Ogdensburg makes no warranties, either expressed or implied, with regard to software obtained from the system.

F. Personal communications

(1) When not representing the City or acting within the scope of their employment duties, users who publish personal or professional opinions must not invoke their City title nor make any representation on behalf of the City of Ogdensburg.

(2) The City of Ogdensburg reserves the right to change its policies and rules at any time. The City of Ogdensburg makes no warranties (expressed or implied) with respect to Internet service, and it specifically assumes no responsibilities for:

- The content of any advice or information received by a user outside City of Ogdensburg employment or any costs or charges incurred as a result of seeking or accepting such advice.
- Any costs, liabilities or damages caused by the way the user chooses to use his/her City of Ogdensburg Internet access.
- Any consequences of service interruptions or changes, even if these disruptions arise from circumstances under the control of the City of Ogdensburg. The City of Ogdensburg's Internet services are provided on an as is, as available, basis.

G. Enforcement and Violations

(1) This policy is intended to be illustrative of the range of acceptable and unacceptable uses of the Internet facilities and is not necessarily exhaustive. Questions about specific uses related to security issues not enumerated in this policy statement and reports of specific unacceptable uses should be directed to the IT Administrator. Other questions about appropriate use should be directed to your Department Head.

(2) The City of Ogdensburg will review alleged violations of the Internet Acceptable Use Policy on a case-by-case basis. Clear violations of the policy, which are not promptly remedied, will result in termination of Internet services for the person(s) at fault and referral for disciplinary actions as appropriate.

(3) All City employees shall sign a City of Ogdensburg Network and Internet Acceptable Use Policy User Agreement.

§ AR-88. COMPUTER SYSTEM SECURITY BREACH NOTIFICATION POLICY

A. Purpose

(1) The Computer System Security Breach Notification Policy is intended to establish procedures to follow in the event a person(s) has acquired without valid authorization, private information of individuals from the records of the City of Ogdensburg and to alert said individuals to any potential identify theft as quickly as possible so that they may take appropriate steps to protect themselves from and remedy any impacts of the potential identity theft or security breach.

(2) This policy is consistent with the State Technology Law, Section 208 as added by Chapters 442 and 491 of the laws of 2005. This policy requires notification to impacted New York residents and non-residents. The City of Ogdensburg values the protection of private information of individuals. The City of Ogdensburg is required to notify an individual when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Security Breach and Notification Act and this policy.

(3) The City of Ogdensburg, after consulting with NYS Office of Information Technology Services (ITS) to determine the scope of the breach and restoration measures, shall notify an individual when it has been determined that there has been, or is reasonably believed to have been, a compromise of private information through unauthorized disclosure.

(4) A compromise of private information shall mean the unauthorized acquisition of unencrypted computerized data with private information.

a. "Private information" means personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

1. social security number
2. driver's license number or non-driver identification card number; or,
3. account number, credit or debit card number, in combination with any required security code, access code or password which would permit access to an individual's financial account.

b. "Private information" does not include publicly available information that is lawfully made available to the general public from City records.

c. This Policy also applies to information maintained on behalf of the City of Ogdensburg by a third party.

B. Permitted Delay

(1) Notification pursuant to this Policy may be delayed if a law enforcement agency determines that notification could impede a criminal investigation. The notification must be made after the law enforcement agency determines that notification would not compromise any criminal investigation.

C. Method of Notification

(1) The required notice must be directly provided to the affected individuals by one of the following methods:

a. written notice;
b. electronic notice, provided that the person to whom notice is required to be provided has expressly consented to receiving notice in electronic form and a log of each electronic notification is kept by the City; and provided further that no person or business may require a person to consent to accepting notice in electronic form as a condition of establishing any business relationship or engaging in any transaction;
c. telephone notification, provided that a log of each telephone notification is kept by the City; or,
d. substitute notice, if the City demonstrates to the State Attorney General that the cost of providing notice would exceed $250,000 or that the number of individuals to be notified exceeds 500,000 or the City does not have sufficient contact information. Substitute notice must include all of the following:

1) e-mail notice, when the City has an e-mail address for the subject persons;
2) conspicuous posting of the notice on the City's Website page if the City maintains one; and,
3) notification to major state-wide media.

D. Information Required

(1) Regardless of the method by which notice is provided, the notice must include contact information for the City and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information were, or are reasonably believed to have been, acquired.

E. Notification of Agencies

(1) Whenever any New York State residents are to be notified pursuant to this Policy, the City must notify the State Attorney General, the Consumer Protection Board and the NYS Office of Information Technology Services (ITS) as to the timing, content and distribution of the notices and the approximate number of affected people. Such notice must be made without delaying notice to affected individuals.

(2) Whenever more than 5,000 New York State residents are to be notified at one time, the City must also notify consumer reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected people. Such notice must be made without delaying notice to affected individuals.

§ AR-89. CYBER SECURITY POLICY (CSP)

A. Purpose

(1) The purpose of the cyber security program is to maintain the confidentiality, integrity and availability of City IT Resources and City data.

B. Chief Information Security Officer

(1) The IT Administrator is responsible for creating and maintaining a cyber security program. In addition, the IT Administrator, or a designee, is responsible for leading the investigation of and response to cyber security incidents. The response to any incident will be developed in collaboration with the Contracted IT Technician.

C. Users

(1) City IT Resource users are responsible for protecting the security of all data and IT Resources to which they have access. This includes implementing appropriate security measures on personally owned devices which access City IT Resources. In addition, users are required to keep their accounts and passwords secure in compliance with the City's Network & Internet Acceptable Use Policy.

(2) City employees may request IT Resource guest access to third parties (e.g., vendors, presenters, etc.) by using the Request for Network Access for Non-City employees form.

D. Network Management

(1) The Contracted IT Technician and IT Administrator are responsible for planning, implementing and managing the City network, including wireless connections.

(2) The following network appliances cannot be implemented at the City without prior written approval by the Contracted IT Technician and IT Administrator:

- Routers
- Switches
- Hubs
- Wireless access points
- Voice over IP (VOIP) infrastructure devices
- Intrusion detection systems (IDS)
- Intrusion prevention systems (IPS)
- Virtual Private Networking (VPN)
- Consumer grade network technologies
- Other networking appliances that may not be included in this list

E. System Administration

(1) The City's expectation is that every City owned IT Resource will be professionally managed by the Contracted IT Technician.

(2) The Contracted IT Technician is responsible for proper maintenance of the system. Negligent management of a City owned IT Resource resulting in unauthorized user access or a data breach may result in the loss of system administration privileges.

(3) System administration responsibilities for all City owned IT Resources, including those that are self-administered, include the following:

- Complying with all applicable City IT policies and procedures
- Working with the IT Administrator to establish the following:
    - Performing an annual cyber security self-assessment for the set of IT Resources administered
    - Installing an appropriate endpoint security/management agent(s)
    - Establishing an appropriate backup strategy and performing regular system backups
    - Regularly updating the operating system and other applications installed on the machine
    - Using, where possible and practical, central City IT services for system login and account management (e.g. Active Directory)

F. Scope:

(1) All City IT Resource users and all City IT Resources are covered by this policy.

G. Policy Terms

Endpoint - Laptop computers, desktop computers, workstations, group access workstations, USB drives and personal network attached storage.

City IT Resources – City owned computers, networks, devices, storage, applications, or other IT equipment. "City owned" is defined as equipment purchased with City funding (including sources such as grant funds, etc.)

H. Procedures

(1) Incident Reporting

a. If a City IT Resource user suspects that a security incident has occurred or will occur, they should report the suspicion immediately to the IT Administrator.

b. Any City IT Resource user who has identified any of the following security events should report the suspected security event to the City IT Administrator:

- Any occurrence of a compromised user account
- Any breach or exposure of sensitive data
- Any occurrence of a server infected with malware
- Three or more simultaneous occurrences of endpoints infected with malware
- Any other instance of malware or suspected intrusion that seems abnormal

I. Enforcement

(1) Violations of this policy may result in loss of City system and network usage privileges, and/or disciplinary action, up to and including termination as outlined in applicable City policies.

(2) All City employees shall sign a City of Ogdensburg Cybersecurity Policy User Agreement.

§ AR-90. TECHNOLOGY EQUIPMENT DISPOSAL POLICY

A. Purpose

(1) The purpose of this policy is to define the guidelines for the disposal of technology equipment and components owned by the City of Ogdensburg ("City"). Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible

and in some instances required by law. In addition, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of City data, some of which is considered sensitive. In order to protect the City's data, all storage mediums must be properly erased before being disposed. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

B. Scope

(1) This policy applies to any computer/technology equipment or peripheral devices that are no longer needed within the City including, but not limited to the following: personal computers, servers, hard drives, laptops, mainframes, smart phones or handheld computers (i.e., Windows Mobile, iOS or Android-based devices), peripherals (i.e., keyboards, mice, speakers), printers, scanners, typewriters, compact and floppy discs, portable storage devices (i.e., USB drives), backup tapes and printed materials.

(2) All City employees and affiliates must comply with this policy.

C. Policy - Technology Equipment Disposal

- When technology assets have reached the end of their useful life they should be sent to the IT Administrator for proper disposal.
- The IT Administrator or designee will securely erase all storage mediums in accordance with current industry best practices.
- All electronic drives must be removed and rendered unreadable (drilling, crushing or other demolition methods).
- All computer equipment should be disposed of properly according to current state disposal regulations.
- Computer equipment refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage device, network switches, routers, wireless access points, batteries, backup tapes, etc.
- Prior to leaving City premises for disposal, all equipment must be removed from the Information Technology inventory system.
- No computer or technology equipment may be sold to anyone without prior approval of the City Manager and the IT Administrator, and then only through the process identified in the Ogdensburg Municipal Code Administrative Regulations, Article V, Sale of City Property, § AR-33, Surplus property.

D. **Policy Compliance**

(1) Compliance Measurement

- The IT Administrator will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits and feedback to the policy owner.
- Exceptions - any exception to the policy must be approved by the City Manager and IT Administrator in advance.
- Non-Compliance - an employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

(2) All City employees shall sign a City of Ogdensburg Technology Equipment Disposal Policy User Agreement.

§ AR-91. NETWORK ACCESS FOR NON-CITY EMPLOYEES

A. Purpose

(1) The purpose of this policy is to protect against unauthorized access to or use of the City of Ogdensburg's information that could result in substantial harm or inconvenience, and to protect against any anticipated threats or hazards to the security and/or integrity of the City's network information.

B. Policy

(1) The appropriate City department will complete a Request for City of Ogdensburg Network Access for Non-City Employees or Contractors and submit the completed form to Contracted IT Technician one week prior to request.

(2) Each Non-City Employee or Contractor shall be subject to and shall abide by the Internet Technology Policies of the Code of the City of Ogdensburg.