

## **Section 17. Technology Use Policy**

### **A. Overview**

The availability of electronic communications technologies has created great opportunities for both business and government. This technological tool will enhance the ability of the City of Waupaca to deliver top quality services to the public. Providing this technology to City employees will promote efficiency and creativity. Access to and use of the Internet and e-mail is vital to perform day to day job duties.

The City of Waupaca promotes the use of resources to improve job performance through Internet and e-mail utilization. Unfortunately, these same technologies can create situations that are not in the best interest of the City organization.

Employees are given computers, e-mail, voice-mail and Internet access to assist them in the performance of their jobs. Employees should have no expectation of privacy in anything they create, store, send or receive using the City's computer equipment. The computer network is the property of the City and may be used only for City business, or other purposes approved and authorized by the City, in compliance with this and other City policies.

The following policy is meant to clarify City administrations' expectations concerning the use of the Internet and e-mail by establishing guidelines for their use.

### **B. General Statements of Policy**

- a. City Staff are expected to use the Internet and E-mail in a responsible manner.
- b. Use of the electronic resource is a privilege and not a right.
- c. Internet and e-mail uses are to be related to the program and operation of the City.
- d. All e-mail accounts are owned by the City. Therefore, the contents of all e-mail communications are accessible at all times by City of Waupaca management for any business purpose.
- e. Use of the City's computer equipment and related technologies is considered consent by the user to have such information monitored by the City with or without prior notice to the user. Employees should have no expectation of privacy in their use of any of the City's computer equipment or technology.
- f. Unauthorized use of copy written material and material protected by trade secret is prohibited.

- g. Use of City equipment, Internet services and e-mail for personal gain/commercial activity is not permitted.
- h. The Internet and e-mail systems should not be considered a secure network and should not be relied on for the transmission of confidential or sensitive data or messages.

**C. Access**

It shall be at the discretion of the Department Head and/or City Administrator to determine which employees in their department(s) shall gain Internet access. Department Heads shall determine and monitor, which uses are appropriate.

**D. Personal Use of E-Mail**

Personal use of the City's computer hardware, software and e-mail capabilities is permitted during breaks, as well as before and after work hours. It is recognized that incidental and occasional personal use of e-mail may occur. Occasional use is permitted and will be treated in the same manner as personal phone calls. Department heads will determine if personal usage is excessive, and if so, take appropriate disciplinary action.

**E. E-Mail Accounts**

City staff who have the need to send or receive e-mail as part of their job duties will be provided with and required to use a city e-mail account. Exceptions of using this account would be during a temporary e-mail outage or other related problem preventing use of said e-mail account. Library staff is served by OWLS for e-mail service and will be subject to OWLS policy regarding e-mail use. To meet open records laws all messages sent and received by city e-mail accounts will be archived.

City staff who have an e-mail account are required to keep the account secure with a strong password.

Employees are prohibited from accessing other employees e-mail accounts, with exception for the following reasons:

- Department Heads or the City Administrator may request access to any subordinates e-mail accounts through the IT department. This could be for an open record request, investigation into communications sent through our e-mail system or to meet day to day operations.
- With department head approval an employee's e-mail account may be accessed for the purpose of finding a specific e-mail to meet day to day operations.

Upon employee termination the IT department will work with the employee's supervisor to disable, forward or provide access to an e-mail account to ensure all communication is received. Terminated employees e-mail accounts will be expected to be disabled within an appropriate period of time.

#### **F. Forbidden Content/Activities**

Employees shall not use the Internet and e-mail in a way that is inconsistent with current policy and procedures. Pornographic, profane, insulting, disruptive or offensive language and graphic material is expressly forbidden, to include screensavers and wallpaper. Other examples include dirty jokes, ethnic slurs, unwelcome propositions, cartoons or love letters.

#### **G. Passwords and System Security**

Many city owned computers have access to privileged data such as employee information, customers lists, financial information or criminal justice data and need proper protection to prevent unauthorized access. Unless higher standards are specified by outside regulation (example being CJIS Policy for the Police Department) computers that access privileged data (as specified by the IT department or City Administration) will need to meet the following requirements:

- Each employee will be assigned their own user account.
- Computer must be locked or logged off during long absences from employees workstation (example: lunch break or away from the office part of the day) and should be locked or logged off at the end of each workday.
- Employee's user account should have a strong password that is changed a minimum of twice annually. The password must be a minimum of eight characters and meet complexity requirements. Employees are suggested to contact the IT department for examples of easy to remember, yet, secure passwords.
- Employees are prohibited from the unauthorized use of the passwords of other employees to gain access to the other employee's computer resources.
- Employees should immediately report to the IT department if they believe that unauthorized users have obtained or accessed an employee's user account or password. If the IT department feels that a user account has been compromised immediate action will be taken to disable or change the password of that account.
- Department Heads and supervisors will immediately inform the IT department of all employee separations before or immediately after so all users accounts and access to city resources are disabled.

#### **H. Remote Access**

Employees may need remote access to their computers or network resources from an off-site location for various reasons to perform their job duties. Employees needing this

access are required to go through the IT department to have this access set up. There are various remote access methods and the IT department will put into place the best method to meet the employee's request. The IT department needs to keep track of all remote access to our network to ensure proper security and employees should not setup remote access without IT department authorization.

**I. Technology Disposal**

Any old technology items (computers, copier printers, thumb drives, cell phones, etc.) that are at the end of their useful life, are on lease and are being returned or being repurposed for non-city use should be wiped cleaned and reset to default settings. This will prevent unauthorized access to city data. If a department is unsure how to do this properly please contact the IT department to have this step performed.

**J. Software Installation**

All software installed on any city owned computers requires the approval of the IT department or employee's department head. The IT department installs and will provide all needed software for employees to perform their job duties. Software is installed and configured in a manner to obtain optimal computer performance. The IT department is also responsible for ensuring proper software licensing and maintains a repository of all software installed for future reinstallations. The IT department will monitor what software is installed and remove any unauthorized programs.

**K. Network/Wireless Access**

The city maintains two computer networks; our internal business network and a public access network. Employees are prohibited from connecting any devices to the internal business network without IT department authorization. Employees wishing to connect devices for internet access such as cell phones, tablets, personal laptops or allowing public visitor's access are required to use our public access wireless network.

**L. Data**

All data, whether on a server or on a workstation is the property of the City of Waupaca. It is against the policy of the city for an employee to purposely delete or modify the work product of another employee without the consent of that employee or their supervisor. Much of the data on the City of Waupaca's computer network is confidential. The release of city data to third parties shall be governed by applicable laws and policies.

Employees are discouraged from storing personal data on city computers and servers. While the IT department is not active in searching for non-city data, upon its discovery, if it is causing stress on network or server resources it will be removed. The city is not responsible for the safekeeping of any non-city data.

All servers and workstations that are fully managed by the IT department are included in the city's backup and disaster recovery plan. It is recommended that employees and department heads work with the IT department to ensure all departmental data and servers are backed up for recovery purposes.

## **M. Viruses**

Virus infection is one of the most well documented threats of Internet use. It is important that employees scan all incoming files for viruses, whether downloaded or attached to electronic mail messages. Users should not open or attempt to read any files received over the Internet that they did not specifically request, and should immediately contact the IT department upon receiving a non-requested file.

## **N. Violations of Policy/Disciplinary Action**

Violations of these procedures and policy will result in appropriate disciplinary action up to and including oral & written reprimand, suspension without pay and discharge.

## **Section 18. Computer Laptop/Tablet Usage Policy**

BACKGROUND: The City of Waupaca can benefit by integrating laptop computers and tablets into City operations. Use of laptops and tablets by city employees and Common Council members leads to more efficient use of resources.

### **1. Policy Goals to be accomplished through use of laptops.**

- a. Improving communication among and between the Common Council, City staff, City residents and businesses.
- b. Reduce the use of paper, photocopies and related office equipment and their associated costs of operation.
- c. Improve the efficiency of putting together the monthly committee and council meeting packets and the meetings themselves.
- d. To make the City organization, policy makers and staff more technology proficient, thereby reaping the cost savings derived from greater efficiency.

**2. Ownership.** The laptops shall be the property of the City of Waupaca and as such maintained by the City. "Maintained" includes costs of software upgrades, hardware repair or replacement and training for new users. Each laptop shall be inventoried and supplied a fixed asset control number.

Common Council members who choose to use a laptop will be provided one at no charge. The laptop will be equipped with software needed to perform City Council duties. The council member is free to use the laptop for both City and non-City related purposes.

Common Council members and City employees may have the option to "buy out" their laptop/tablet when it is replaced or upon separation from the City with administration

approval. For purposes of this policy, laptops/tablets will be amortized over four (4) years. Beyond that, if the laptop/tablet still meets minimum acceptable standards specified by the IT department the buy-out cost will be 10% of the original purchase price. Before buy-out can occur the laptop will first be inspected by the IT department to remove any licensed software and confidential city data.

If the equipment is not surrendered to the City at time of separation, then any cost owed to the City by the council member or employee shall be billed the outstanding amount owed, granting the individual a reasonable amount of time to make full payment. If the City is unable to collect the funds, the City reserves the right to pursue repayment through all available means.

3. Accessory Equipment. Common Council members and City staff shall have the opportunity to purchase accessory equipment for their laptop not approved for payment by the City but must do so at their own cost. The equipment shall remain the property of the council member or employee. The City is not responsible for the care and maintenance of this equipment. The City's IT department should be made aware of these proposed purchases to ensure the additional equipment and/or software is compatible.

4. Internet Services. It shall be the responsibility of the council member and staff employee to retain their own Internet service provider at their cost. However, when in City Hall the individual will have internet access available.

5. Policy Acceptance by council Member and City Staff. Each Common Council member and City staff issued a laptop will be required to sign a statement that they have read and understand this policy.

6. Monitoring Responsibility. The City administrator's office, working through the City's IT Department, shall have the responsibility for ensuring that this policy is adhered to.

7. Effective Date. This policy shall become effective upon adoption by the Waupaca Common Council.

**Adopted By Council on: January 21, 2014**