

TOWN OF YACOLT  
RESOLUTION #572

AMENDING RESOLUTION #552 TOWN POLICY FOR ELECTRONIC DEVICE USAGE FOR EMPLOYEES AND ELECTED OFFICIALS MARKED AS ATTACHMENT A ELECTRONIC DEVICES POLICY.

**WHEREAS:** The Town Council of the Town of Yacolt, Washington is in regular session this 4<sup>th</sup> day of September; and

**WHEREAS:** The members of the Town Council have had notice of the time, place, and purpose of said meeting; and

**WHEREAS;** It is important to have clear policies in place detailing the guidelines for appropriate behavior for employees and elected/town officials; and

**WHEREAS:** the Town Council wishes to have a clear policy in effect for the usage of and passwords for wireless internet systems and town assigned electronic devices by elected/town officials and employees; and

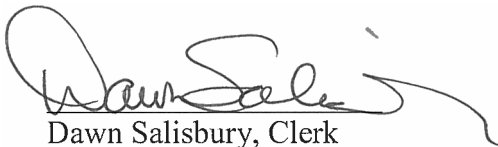
**WHEREAS;** such policies brings the Town of Yacolt in compliance with the auditing requirements of the State Auditor's Office;

**NOW THEREFORE, BE IT RESOLVED,** that the Town Council of the Town of Yacolt, Washington do hereby adopt the attached policy marked as Attachment A Electronic Device Policy as the official policy regulating the usage of the wireless internet, email, messaging and other forms of communication with electronic devices owned by the Town of Yacolt; and

**BE IT FURTHER RESOLVED** that a receipt acknowledgement form shall bear the signature from each employee or town official who is assigned an electronic device and such document shall be kept by the Town Clerk in a file of records and further resolves that Resolution #572 shall become effective upon the date of adoption by the Town Council of Yacolt, Washington on this 4<sup>th</sup> day of September, 2018.

APPROVED this 4<sup>th</sup> day of September, 2018.

Attest

  
Dawn Salisbury, Clerk

Town of Yacolt

  
Vince Myers, Mayor



# Town of Yacolt

P. O. Box 160

202 W. Cushman St.

Yacolt, WA 98675

(360) 686-3922 FAX (360) 686-3853

[www.townofyacolt.com](http://www.townofyacolt.com)

## **Town of Yacolt Electronic Device Policy for Elected Officials and Employees**

**TITLE: Wireless Internet, email, instant messaging and other communication devices for Town Council members and employees.**

**PURPOSE:** The Town of Yacolt provides a wireless Internet system (“Wi-Fi”) for use in Town Council chambers for the purpose of providing an effective method to communicate, preform research and obtain information that will assist in performing Town Council related tasks.

The purpose of this policy is to provide guidelines on appropriate use, care and requirements of Town-provided wireless Internet and to provide basic information on the appropriate use of Town-issue or personal communication devices on that Wi-Fi system and other Wi-Fi systems.

**POLICY:** It is the policy of the Town of Yacolt to adhere to the Revised Code of Washington (RCW) 42.30 regarding Open Public Meetings and RCW 42.56 regarding public records.

- 1) Council members and employees are expected, and have the obligation, to use good judgement when using the Internet and electronic communication tools while in a Town Council session. It is strongly recommended that council members and employees only use Town provided Wi-Fi in council chambers to access information related to Town business from the Town of Yacolt website.(townofyacolt.com) Should a council member have an issue with access to Wi-Fi services in council chambers, they should notify the Town Clerk.
- 2) All electronic devices connected to the Town’s Wi-Fi system shall be turned off during closed executive sessions. Elected officials, by virtue of their position, are privilege to confidential information that could not otherwise be obtained by the general public. Pursuant to RCW 42.23.070 – Code of Ethics for Municipal Officers, Prohibited Acts – no municipal officer may disclose confidential information gained by reason of the officer’s position, nor may the officer otherwise use such information for his or her personal gain or benefit.
- 3) All records, regardless of format, related to the conduct of Town business reviewed, created, or altered must be retained per the State of Washington Local Government

Common Records Retention Schedule, (the CORE manual), pursuant to RCW 42.56 and RCW 40.14, Preservation and Destruction of Public Records.

- 4) The Town reserves the right to access, monitor and disclose the contents of electronic messages and any record, regardless of format, related to the conduct of Town business on Town-issued or personal devices that council members and employees use to access the Town Wi-Fi system. Council members and employees should have no expectation of privacy in either sending or receiving electronic messages, or other information on the Internet, Town network or other electronic media.
- 5) All electronic messages, Internet and network activity must be appropriate to the Town's professional environment and consistent with the Town's policies prohibiting discrimination and harassment.
- 6) Per state law, all documents, files, communications and messages created, reviewed or altered that are related to the conduct of Town business, regardless of format, are property of the Town. As a result, these documents, files communications and messages are not private or confidential unless otherwise noted in the Revised Code of Washington.
- 7) Technology resources may be used for incidental personal needs as long as such use does not result in, or subject the Town to, additional costs or liability; interferes with business, productivity, or performance; pose additional risk to security, liability or privacy; cause or tend to cause damage to Town's reputation or credibility. Incidental, personal usage should generally conform to limits typically associated with personal phone calls.

This document does not attempt to address every possible situation that may arise. Professional judgement, etiquette and common sense should be exercised while using Town resources. Anything stored on Town's devices/accounts are not subject to privacy.

- 8) The Town recognizes that public Internet communications technologies are effective tools to promote community and government interaction, and that council members and employees want to participate in public communication. This includes blogging, discussion forums, social networking, message boards, e-mail groups and other media that are now commonplace tools by which people share ideas and information. While all forums are not encouraged, all such information is subject to public records requests. However, since activities on public Internet communication sites are electronically associated with Town network; addresses and accounts that can be easily traced back to the Town of Yacolt, the following rules must be followed for participation on these interactive public Internet communication sites:
  - a. When expressing council member's or employee's view, make it clear that it does not necessarily represent the view of the Town of Yacolt. Opinions or views other than those reflective of Town policy must contain the following disclaimer: "The content of the electronic communication does not necessarily reflect the official views of the elected officials or citizens of the Town of Yacolt."

- b. Always protect the confidentiality, integrity, and availability of all critical information.
  - c. Council members and employees must not post any material that is obscene, defamatory, profane, libelous, threatening, harassing, abusive, hateful, or embarrassing to or of any other council member, employee, person, and/or entity.
  - d. To protect council member's and employee's privacy and the privacy of others, phone numbers or email addresses must not be included in the content body.
  - e. The Town provides council members and employees access to and support of the Exchange/Outlook messaging (e-mail) system. Access or usage of any other messaging systems is not allowed unless it is web based.
- 9) Because electronic messages can be retrieved even after deletion by the author or recipient, and are not confidential, users should treat each electronic message as they would a hard copy that would potentially be distributed to everyone in the Town and subject to discovery in a legal proceeding.
- 10) All council members and employees with access through the Town facilities are responsible for complying with the guidelines contained in this policy. Violations may result in revocation of access privileges. Criminal and/or civil penalties or other legal action against a council member or employee is a possibility depending upon the action.
- 11) The following is a list of prohibited uses:
- a. Transmitting any material or messages in violation of Federal, State, Local law, Ordinance, Regulation or Town policy.
  - b. Taking action via electronic device while in an open public meeting of the governing body. "Action," as defined under RCW 42.30.020, means the transaction of the official business of a public agency by a governing body including, but not limited to, receipt of public testimony, deliberations, discussions, considerations, reviews, evaluations, and final actions. "Final action" means a collective positive or negative decision, or an actual vote by a majority of the members of a governing body when sitting as a body or entity, upon a motion, proposal, resolution, order, or ordinance.
  - c. Anything that may be construed as harassment or disparagement of other based on race, national origin, sex, sexual orientation, age, disability, or religious beliefs will not be tolerated. This includes, but is not limited to, sending threatening messages, slurs, obscenities, sexually explicit images, cartoons or messages.
  - d. Distributing sensitive or confidential information, per RCW 42.23.070, Code of Ethics for Municipal Officers, Prohibited acts.
  - e. Installing client based software.
  - f. Downloading personal documents or attachments. Video streaming, gambling sites, sports, music videos, personal dating sites, and downloading software for personal use not approved by the Mayor or Town Clerk.

- g. Distributing unauthorized broadcast messages, soliciting or proselytizing others for commercial ventures, religious or political causes, or other non-job related matters except as provided elsewhere in this policy.
- h. Accessing or distributing offensive or pornographic materials.
- i. Using Town-provided Wi-Fi for personal use, to accomplish personal gain, or to manage a personal business.
- j. Downloading or distributing copyrighted materials not owned by the Town including software, photographs, or any other media except when authorized by the Mayor or Town Clerk as it pertains to work related issues.
- k. Developing or distributing programs that are designed to infiltrate computer systems internally or externally (viruses) or intentionally disrupting network traffic or crashing the network and connected systems.
- l. Accessing or downloading any resource for which there is a fee without prior appropriate approval.
- m. Representing yourself as another user or employee, forging electronic mail messages, unauthorized access of others' files with no substantial business, or vandalizing the data of another user.
- n. Attempting to access any system, which a council member or employee is not authorized to access. (hacking)
- o. Giving your user name and password to anyone, except the Town Clerk or designee for any purpose.
- p. Inappropriate use, which is determined by the Town to be a violation of the intended purpose of any electronic media.

12) Users should be attentive to emails that may have unusual or questionable subject lines to mitigate spam, phishing scams and script born viruses that come into the network through email attachments or by clicking on links that lead to hostile web sites. If you suspect phishing scams or script born viruses in email attachments immediately contact the Town Clerk.

13) The Town will assign an initial password for access to the assigned device. Each user is responsible for immediately changing the password(s) for their assigned device. The users will write their password on a 3x5 index card which will then be sealed in an envelope such that it cannot be read from the outside. The envelope will be turned over to the Town Clerks office where it will be placed in the Town safe for emergency use. The use of another user's account or attempt to capture other users' passwords is prohibited. Each user is responsible for restricting unauthorized access to the network by locking their computer or logging out of their computer account when leaving their computer unattended. Council members and employees who discover unauthorized use of their accounts must immediately report it to the Town Clerk.

14) The Town of Yacolt will take the necessary steps to protect the confidentiality, integrity, and availability of all of its critical information. Critical information is defined as information which if released could damage the Town financially; put council members and employees at risk; put facilities at risk; or could cause legal liability. Examples of critical data include: employee health information, social security numbers, credit card holder information, banking information, police crime investigation, etc.

- a. Council members and employees with access to critical information are responsible for its protection. Council members and employees must take reasonable steps to ensure the safety of critical information including: avoiding putting critical data on laptops; encrypting data at any time it is electronically transported outside the Town network; not storing, saving, or transmitting critical data to a home computer or other external computer; ensuring inadvertent viewing of information does not take place; and destroying or rendering the information unreadable when done with it.
- b. Council members and employees should not transport critical data on unencrypted devices such as thumb drives, CD's, or Smartphones.
- c. The city will restrict access to critical information only to council members and employees who have a legitimate business need-to-know. Each system owner is responsible for keeping an inventory of critical information and ensuring that access to it is limited.
- d. Council members and employees will be assigned unique user IDs and passwords for network access. Access to systems and applications containing critical information will only be allowed via unique user IDs. Access will be monitored and actions will be traceable to authorized users.

15) The Town also needs to be able to respond to proper requests resulting from legal proceedings that call for electronically-based evidence. Therefore, the Town must, and does, maintain the right and the ability to enter into any of these systems and to inspect and review any and all data recorded in those systems. Because the Town reserves the right to obtain access to all electronic mail messages left on or transmitted over these systems, council members and employees should not assume that such messages are private and confidential or that the Town or its designated representatives will not have a need to access and review this information. Council members and employees that access Town Wi-Fi during a council meeting, whether on a private electronic device or Town-issued business equipment should also have no expectation that any information stored on their computer – whether the information is contained on a computer hard drive, computer disks or in any other manner – will be private.

The Town reserves the right to regularly monitor electronic mail messages, information, and all documents. The Town will inspect the contents of computers or electronic mail in the course of an investigation triggered by indications of unacceptable behavior or as necessary to locate needed information that is not more readily available by some other less intrusive means. A council member's or employee's rights while accessing the Internet by use of the Town's property/account does not include the right to privacy. The contents of computers and electronic mail, properly obtained for some legitimate business purpose, may be disclosed by the Town if necessary within or outside of the Town.

- 16) The council member or employee the device is assigned to is liable for all damages incurred (dropping etc.) other than normal wear and tear.
- 17) Council members and employees are required to return devices at the end of term or termination of employment, or he/she will be required to reimburse the town for the cost of the device.

- 18) Legal council may review any request for access to the contents of an individual's electronic device prior to access being made without the individual's consent.
- 19) Any council member or employee who violates this policy for improper uses may be subject to revocation of privileges.
- 20) All council members and employees are required to work collaboratively with the Town Clerk's Office for access to a personal or Town-issued electronic device when responding to a public records request.

*"The Town of Yacolt celebrating 109 years--1908-2017"*