City of Ferndale

City Facilities Wi-Fi Policy for Elected Officials

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

PURPOSE: The City of Ferndale provides a wireless Internet system ("Wi-Fi") for use in City Council chambers for the purpose of providing an effective method to communicate, perform research and obtain information that will assist in performing City Council related tasks.

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

POLICY: It is the policy of the City of Ferndale 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 are expected and have the obligation to use good judgment when using the Internet and electronic communication tools while in a City Council session. It is strongly recommended that council members only use City-provided Wi-Fi in council chambers to access information related to City business from the City of Ferndale website (cityofferndale.org). Should a council member have an issue with access to Wi-Fi services in council chambers, they should notify the City Clerk.

2) All electronic devices connected to the City'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 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 City business reviewed, created or altered must be retained per the State of Washington Local Government Common Records Retention Schedule. (the CORE manual), pursuant to 42.56 RCW and 40.14 RCW, Preservation and Destruction of Public Records.

4) The City reserves the right to access, monitor and disclose the contents of electronic messages and any record, regardless of format, related to the conduct of City business on City-issued or personal

devices that council members use to access the City's Wi-Fi system. Council members should have no expectation of privacy in either sending or receiving electronic messages, or other information on the Internet, City network or other electronic media.

5) All electronic messages, Internet and network activity must be appropriate to the City's professional environment and consistent with the City'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 City business, regardless of format, are property of the City. As a result, these documents, files, communications and messages are not private or confidential unless otherwise noted in the Revised Code of Washington.

7) 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 City and subject to discovery in a legal proceeding.

8) All officials with access through the City facilities are responsible for complying with the guidelines contained in this policy. Violations may result in revocation of access privileges. Because access to this Wi-Fi system will be a public offering, removal of privileges by one official may mean the entire system is no longer provided publicly, thus causing all to lose access. Criminal and civil penalties or other legal against an official is a possibility depending upon the action.

9) The following is a list of prohibited uses.

The following is a list of prohibited uses:

a) Transmitting any material or messages in violation of Federal, State, Local law, Ordinance, Regulation or City 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 others based on race, national origin, sex, sexual orientation, age, disability, or religious or political 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) 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.
f) Accessing or distributing offensive or pornographic materials.
g) Using City-provided Wi-Fi for personal use, to accomplish personal gain, or to manage a personal business.
h) Downloading or distributing copyrighted materials not owned by the City, including software, photographs, or any other media except when authorized by the City Administrator or Department Head as it pertains to work related uses.
i) 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.
j) Accessing or downloading any resource for which there is a fee without prior appropriate approval.
k) Representing yourself as another user or employee, forging electronic mail messages, unauthorized access of others' files with no substantial business purpose, or vandalizing the data of another user.
l) Attempting to access any system, which an employee is not authorized to access (hacking).
m) Giving your user name and password to anyone, except the System Administrator, City Clerk or designee for any purpose.
n) Inappropriate use, which is deemed by the City to be a violation of the intended purpose of any electronic media.

10) The City also needs to be able to respond to proper requests resulting from legal proceedings that call for electronically-stored evidence. Therefore, the City 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 City reserves the right to obtain access to all electronic mail messages left on or transmitted over these systems, Council members should not assume that such messages are private and confidential or that the City or its designated representatives will not have a need to access and review this information. Council members access City Wi-Fi during a council meeting, whether on a private electronic device or City-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 City reserves the right to regularly monitor electronic mail messages, information and all documents. The City 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' rights while accessing the Internet by use of the City'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 City if necessary within or outside of the City.

11) Legal Counsel 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.

12) Any council member who violates this policy for improper uses may be subject to revocation of privileges.

13) All council members are required to work collaboratively with the City Clerk's Office for access to a personal or City-issued electronic device when responding to a public records request.