CITY OF TUMWATER
POLICY MANUAL - PART 2: OPERATING POLICIES

SECTION 5
TECHNOLOGY USE

5.01 Purpose

The purpose of this policy is to implement guidelines for the use of the City's technology. This policy sets forth telephone, cell phone, voice mail, computers, all software, and computer-related network resource restrictions. All City communications, both internal and external, should reflect the City's commitment to quality service and the highest degree of professionalism.

5.02 Definitions

"ER&R Program:" the Equipment Rental and Replacement (ER&R) program of the City.

"Information Technology Division:" a division of the Administrative Services Department that services all technology that is in the ER&R program.

"Primary Records:" The original record (whether created or received by the agency) which serves as the official record, and must be retained in accordance with a current approved records retention schedule.

"Sensitive Data:" Information that is protected against unwarranted disclosure.

"Technology:" all City-provided computers and devices or other computers and devices owned by employees but used to store primary records or sensitive data, including laptops, tablets, cell phones, voice mail accounts, pagers, email accounts, software, digital applications (apps), instant messaging services, text messages, social media sites, chat services, Facebook accounts, Twitter streams, blogs, and other websites. It also includes all two-way radios, radio base stations, intercom systems, printers, faxes, scanners, cameras, digital images, cabling, wireless antennas, City-owned conduit, fiber, network, and Wi-Fi resources.

SECTION 5
TECHNOLOGY USE

New types of technology and media are constantly being developed and launched, this policy applies to those technologies and media forms and uses. In this policy, the term "technology" shall mean all of the above.

5.03 Policy

This policy applies to i) all types of technology and media that City employees, officials, and volunteers use during work hours, or ii) work undertaken utilizing hardware, software, technology/media, digital apps, network capabilities, or other resources supplied by the employer, or (iii) technology used while performing tasks related to employment.

Technology resources are made available to City officials, employees, and qualified volunteers. These resources are provided in order to improve communications and information exchange within and from outside the City, other local, state and federal officials, professional and business associates, and to provide information and research resources. Technology resources are intended for official City business purposes. Prohibited uses are set forth in Section 5.04. Exceptions to prohibited uses are those set forth in Section 5.05.

Department Managers reserve the right to review their employee's technology use to determine whether the use of the resources is appropriate and conforms to this policy. If an employee is not complying with this policy, the Department Manager has the choice to remove the employee's access to the technology resources or to proceed with other disciplinary action, up to, and including, termination. The City Administrator or designee reserves the right to review the use of technology resources by Department Managers to determine whether their use is appropriate and conforms to this policy.

All software installations must be approved prior to acquisition by the Information Technology Division of the Administrative Services Department. This is to avoid system conflicts, redundancies, ensure security of system, and to anticipate necessary upgrades to hardware, etc.

The Information Technology Division supports technology systems that are in the ER&R program.

Employees are responsible to establish and maintain passwords consistent with City requirements. User accounts and passwords must be unique to each employee and kept confidential.

SECTION 5
TECHNOLOGY USE

5.04 Prohibited and Inappropriate Use

Technology resources are intended for the conduct of City business. Exceptions to prohibited and inappropriate uses are those permissible uses set forth in Section 5.05. Examples of prohibited and inappropriate use include but are not limited to:

A. Seeking to gain or gaining information for criminal purposes. Seeking access to City passwords belonging to others.

B. Unauthorized attempts to break ("hack") into any computer or voicemail system whether of the City or another organization.

C. Using technology resources or knowingly allowing another to use the resources to advertise or promote a personal business, for commercial product advertisement, for promotion or distribution of information about non-City affiliated organizations when such organizations are unrelated to any activity or professional organization that is necessary for or adjunct to the employee's job or professional certification, or for religious purposes.

D. Using a technology resource to assist a campaign for election of any person to any office or for the promotion of or opposition to any ballot proposition, except as set forth in RCW 42.17.130.

E. Processing, distributing, transmitting, or displaying inappropriate stored electronic media such as obscene, libelous, or defamatory materials. This includes downloading, viewing, transmission and possession of pornographic, profane, or sexually explicit materials.

   Activities of the police department related to criminal investigations, or personnel investigations authorized by a Department Manager, would not constitute a prohibited or inappropriate use.

F. Sending messages that constitute criminal activity, including but not limited to threatening or harassing messages.

G. Sending or posting confidential materials outside of the City, or posting City confidential materials inside the City to non-authorized personnel.

H. Infringing on third party copyrights or other intellectual property rights, license agreements, or other contracts; for example, illegally installing or making available copyrighted software.

I. Utilizing technology resources in a manner that potentially reduces the internet bandwidth available for City business such as streaming media for non-work purposes.

J. Installing unauthorized software such as games, internet based services, or other personal software on City owned equipment.

K. Accessing online gambling websites in order to gamble.

5.05 Permitted Personal Use

Limited use of technology is permitted subject to the following limitations:

A. Such use shall be reasonable, as determined by management, and shall not occur during regularly scheduled employee work hours but is permitted before and after work hours and during scheduled work breaks. Exempt employees that do not have a regular schedule are allowed reasonable use of technology resources.

B. Such use is permitted only to the extent that the City does not incur user charges. Any such charges, except for those approved by the Department Manager, shall be billed directly to the employee.

C. Personal use remains subject to the "prohibited and inappropriate use" policies set forth in Section 5.04.

D. The City provides an electronic bulletin board to employees for their personal use. The bulletin board may be used to sell personal items, post announcements, and for other uses that would not fall within the definition of a prohibited or inappropriate use as set forth in Section 5.04.

5.06 Use and Privacy Caution

Technology users are advised that any communication on publicly-owned equipment or created in the course of an employee's duties is a public record and subject to disclosure under Washington state law. Users should be aware that any technology

resource may be accessible to other users. The employer does not guarantee the privacy or confidentiality of communications using technology resources, whether internal or external. Users should assume that any communication, whether deleted or unsaved, may be retrieved and retained (whether as a "temporary" or backup file, or through some other means). All users should compose communications with the expectation that they could be made public.

The City has the right to monitor, retrieve, read, retain, and/or disclose all such files, data, metadata, and information (temporary, deleted, or otherwise). The employer will access and/or monitor any information or communications created, viewed, or stored using the technology. The employer's access and/or monitoring will occur without notice to employee. The City's retention will occur without further notice to employee.

City will use and/or disclose information or communications created, viewed, or stored using the technology resources for any business purpose, including, but not limited to, investigation, litigation, internal dispute resolution, disciplinary action, personnel decisions, or protection of property. The City's use and/or disclosure may occur without notice to employee.

For personal safety and the safety of others, exercise caution when communicating with others. It is inadvisable to give out personally identifiable information such as your home phone number, your address or credit card numbers through the internet or email.

The following guidelines are established for sending and receiving electronic mail:

A. If you feel uncomfortable about the receipt of any particular email, please discuss it with your supervisor.

B. Do not send angry messages. Take a minute before you enter an email message. Be careful about the words you choose and how you use them. Remember that messages can be printed or forwarded.

C. Be careful when sending replies; make sure that mail is addressed to the individual or group you want to receive it.

D. Email is best for short messages. A message that takes only one screen is more likely to be read. Also, mail takes up space. Learn to use the archive system ant to save messages; otherwise, delete them.

SECTION 5
TECHNOLOGY USE

5.07 Technology Security Protocols and Oversight

Anti-virus software will be running on all computers that are connected to the internet, in order to check files, email, and attachments for embedded viruses.

The Information Technology Division does the routine system administration of all telephone, computers, networks, and servers. This system administration oversight includes monitoring of internet usage by employees according to the policy. All violations discovered through such monitoring shall be reported to the appropriate Department Manager and other necessary City staff. Appropriate action will follow, according to this and other relevant City policies.

As a condition of using the City's technology resources, all employees agree and understand that they have absolutely no expectation of privacy from City management with respect to any information stored on City equipment. Employees are authorized to use passwords to protect their information from access by others, but passwords are not provided as a means of assuring privacy to the employee from access by City management.

5.08 Use of Text Messaging for Conducting City Business

All text messages considered primary records are to be retained in a manner acceptable to the City. Sending text messages on cell phones and other electronic devices (whether owned by the City or not) to conduct City business is allowed only on devices that are enrolled in a text message archive service managed by the Information Technology Division. Employees faced with an emergency situation may use text messaging to conduct business when no reasonable alternative is available, but primary records of messages must be retained in a manner acceptable to the City.