The only personal property that an employee may be asked to use for City business is their personal vehicle. However, employees may choose to bring and use personal property in the performance of job duties. If personal property is used to perform job duties, employees must obtain written approval from a supervisor prior to its use and the property must comply with City standards.

It is the employee's responsibility to safeguard personal belongings. The City will not be liable for lost, damaged or stolen property of its employees and at no time will the City replace or reimburse an employee for personal property that an employee brings to the workplace. Employees are encouraged to exercise reasonable care to safeguard personal items brought to work. For example, employees should not bring valuables to work and should not leave personal items where they might be damaged or stolen.

Improper or excessive use of personal property brought onto City property or worksites or during work hours (for example, the excessive or inappropriate use of personal cell phones for personal phone calls, text-messaging, imaging or videotaping), may also result in disciplinary action, up to and including termination.

9.6. COMPUTER SYSTEM, INTERNET, E-MAIL USE AND PASSWORD POLICIES

9.6.1 The City of Ellensburg furnishes computers for employees to use in conducting City business.

This includes access to e-mail and the Internet. The Internet contains many useful features, including e-mail to non-City resources, access to research materials, and information exchange. The purpose of this policy is to establish basic rules for employees' use of the City's computer system, including the Internet and Internet e-mail.

The Internet can be misused in a variety of ways, including but not limited to:

1) Downloading files that contain viruses, thereby endangering City information services;

2) Accessing objectionable material;

3) Wasting work time by performing unauthorized research or accessing non-business related information and people or for computer games, or online games.

Individual Responsibilities: Internet users are responsible for complying with this and all other City policies when using the City's resources for accessing the Internet. Violation of this policy is grounds for disciplinary action, up to and including termination.

General Policies for Use of the City's Computer System, Including the Internet:

An employee does not have a right to privacy when using the Internet via City resources and employees should not expect or assume any privacy regarding the content of email communications. The City reserves the express right to monitor and inspect the activities of the employee while accessing the Internet at any time, and to read, use and disclose e-mail messages. In addition, all software, files, information, communications, and messages (including e-mails) downloaded or sent via the Internet using City resources are the City's records and property of the City; such records are subject to potential review and disclosure under the public disclosure law of the State of Washington. Even after an email message has been "deleted," it may still be possible to retrieve it.

The City Manager has the right to restrict or prohibit any employee from Internet access for violation of the policies set forth in this section 9.6. Violations may also result in disciplinary action, up to and including termination.

Internet use via City resources is for City business. Except as outlined here, use of City's computer, Internet and email services are for City business only. Some limited personal use is permitted, so long as it does not result in cost to the City, does not interfere with the performance of duties, is brief in duration and frequency, does not distract from the conduct of City business and does not compromise the security or integrity of City information or software. Such limited use shall not occur on "paid time," but is permitted immediately before or after work hours and during an employee's breaks. Examples of allowable personal use include accessing a weather report or news item on the Internet, or transmitting e-mail to a family member to assure safe arrival at home. Any personal use of the City's computer, Internet and email services must comply with all applicable laws and City policies, including anti-discrimination policies and Internet usage policy.

Internet use must comply with applicable laws and City policies including but not limited to all federal and state laws, and City policies governing sexual harassment, discrimination, intellectual property protection, privacy, public disclosure, confidentiality, misuse of City resources, information and data security.

All Internet use must be consistent with the City's Personnel Policies Manual.

The City's computer system permits employees to perform jobs, share files, and communicate internally and with selected outside individuals and entities in the performance and conduct of City business. Employees are prohibited from gaining unauthorized access to another employee's e-mail messages, or sending messages using another employee's password.

In order to prevent potential City liability, it is the responsibility of all Internet users to clearly communicate to the recipient when the opinions expressed do not represent those of the City of Ellensburg.

The City has the capability and reserves the right to access, review, copy, modify and delete any information transmitted through or stored in its computer system. The City may disclose all such information to any party (inside or outside the City) it deems appropriate and in accordance with applicable law. Accordingly, employees should not use the computer system to send, receive or store any information they wish to keep private. Employees should treat the computer system like a shared file system—with the expectation that files sent, received or stored anywhere in the system will be available for review by any authorized representative of the City for any purpose, as well as the public if a proper request is made for public records.

Good judgment should always be employed in using the City's e-mail and Internet systems. Employee e-mail messages may be read by someone other than the person(s) to whom they were sent. E-mail inconsistent with the City's policies must be avoided. For example, it is prohibited to make jokes or comments which could offend someone on the basis of gender, race, age, religion, national origin, disability, sexual orientation, or any other class protected by law. These comments would be in direct conflict with the City's policies prohibiting discrimination and harassment. Accordingly, employees should create and send only courteous, professional and businesslike messages that do not contain objectionable offensive or potentially discriminatory material.

Caution should be taken in transmitting confidential information on the computer system. Employees should use due care in addressing e-mail messages to assure messages are not inadvertently sent to the wrong person inside or outside the City. E-mail creates a written record subject to court rules of discovery and may be used as evidence in claims or legal proceedings. Once sent, e-mail cannot be retracted. Even after deletion at a workstation, e-mail can be retrieved and read.

The safety and security of the City's network and resources must be considered at all times when using the Internet. Any programs from a non-current source (i.e., software that is not purchased in original diskette or CD ROM format) or which involve executable or binary files must not be downloaded or installed without prior permission from the IT Division and the appropriate Department Director and without being properly scanned for viruses. Employees are not to share or reveal individual passwords to anyone other than an authorized member of IT.

There is a wide variety of information on the Internet. Some individuals may find information on the Internet offensive or otherwise objectionable. Individual users must be aware that the City has no control over available information on the Internet and cannot be responsible for the content of information.

Prohibited Uses of the Internet: The following is a non-exclusive list of prohibited uses of the Internet and Internet e-mail:

Commercial use – any form of commercial use of the Internet is prohibited;

Solicitation – the purchase or sale of personal items or non-business items through advertising on the Internet is prohibited;

Copyright violations – the unlawful reproduction or distribution of copyrighted information, regardless of the source, is prohibited;

Discrimination/Harassment – the use of the Internet to send messages or other content which is harassing, derogatory or unlawfully discriminatory to employees, citizens, vendors or customers is prohibited;

Political – the use of the Internet for political purposes is prohibited;

Aliases/Anonymous messages/misrepresentation – the use of aliases or transmission of anonymous messages is prohibited. Also, the misrepresentation of an employee's job title, job description, or position with the City is prohibited;

Social networking sites – the accessing and/or creation of social networking sites, such as MySpace, Facebook, Twitter, Blogs and similar sites is prohibited for non-city business purposes;

Instant messaging;

Misinformation/Confidential Information – the release of untrue, distorted, or confidential information regarding City business is prohibited;

Viewing or Downloading of Non-Business Related Information - the accessing, viewing, distribution, downloading, or any other method for retrieving non-City related information is prohibited. This includes, but is not limited to, entertainment sites, pornographic sites, sexually explicit sites, chat rooms and bulletin boards;

Unauthorized attempts to access another's network or e-mail account;

Display or transmission of sensitive or proprietary information to unauthorized persons or organizations;
Spamming e-mail accounts from the City's e-mail services or City machines.

Nothing in this chapter prohibits the use and access of the described systems for bona fide law enforcement and investigation purposes.

Remote access to the City computing resources and electronic assets must be authorized and granted based upon individual identification and prior management approval.

9.6.2 **Information Technology Password Policy** - Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of the City of Ellensburg's resources. All employees with access to the City of Ellensburg systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purpose of the City of Ellensburg Information Technology Password Policy is to establish a standard for the creation of strong passwords, the protection of those passwords, the frequency of change, as well as define the requirements and standards that the City adheres to. Passwords are the first level of defense on many of the City's systems. Like many organizations that provide Information Technology systems and services to their employees the battle to protect those systems and provide reasonable access is a delicate balance between security and accessibility.

This policy applies to all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any City of Ellensburg facility, has access to the City of Ellensburg network, or stores any non-public City of Ellensburg information.

Employee password requirements are as follows:

- Whenever possible a password history of 15 passwords will be kept in an attempt to prevent the re-use of a password.
- Maximum password age 90 days
- Minimum password length of 8 or more characters
- Password complexity must be a combination including 3 of the following:
    - A Lower case letter
    - An UPPERCASE letter
    - A number
    - A special Character (e.g., !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- A password can't contain your first or last name.

- A password cannot contain your username.

The City of Ellensburg password requirements are based upon Microsoft's best practices for password characteristics, which define how to enforce password history, age, length, and complexity requirements. Employee passwords must meet the following standards:

- All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed on at least a quarterly basis.
- User passwords on systems outside the City's control (e.g., email, web, Software as a Service "SaaS", or other hosted services) must be changed at least every six months and if possible an attempt should be made to adhere to the City's password requirements.

The City of Ellensburg password protection standards are intended to assist employees in preventing password "leakage" resulting in a password being wrongfully accessed or used against the city.

The City also requires employees adhere to the following password protection standards:

- Do not use the same password for City of Ellensburg accounts as for other non-City of Ellensburg access (e.g., personal ISP account, personal web based email accounts, and other online user accounts.)
- Do not share your password/s with anyone else other than authorized City of Ellensburg Information Technology personnel.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Do not reveal your password to anyone over the phone unless you are certain it is in fact an authorized Information Technology City of Ellensburg personnel.
- If someone demands a password, refer them to the City's Personnel Policies or Information Technology personnel.
- Do not write passwords down or store them anywhere (not even in your office).
- Do not store passwords in a file on ANY computer system without encryption.
- Do not hint at the format of a password (e.g., "my family name")
- Do not reveal a password on questionnaires or security forms

9.7. WIRELESS COMMUNICATION DEVICES

Wireless communications devices include, but are not limited to, cellular telephones, wireless handheld devices and pagers. An employee's personal communications using City wireless communications devices should be limited, and employees are expected to exercise sound judgment in both the duration and frequency of such use. These devices should not be treated as if they were the employee's personal property. As with similar