City of Camas
WASHINGTON

TECHNOLOGY RESOURCES USAGE POLICY AND WORK RULES

Purpose

This policy is designed to establish general standards and responsibilities for the acceptable use of City technology resources, which are provided to promote and enhance City services to the public. This policy applies to all users of City Technology resources regardless of employment status. The overall purpose of this policy is to safeguard and protect all such technology resources from anything other than authorized, intended and lawful uses.

Policy

It is the policy of the City to provide managed, secured technology resources to approved users of the network and systems, for purposes which are safe, legal, ethical, and in support of the City's vision and mission; and, which are in compliance with all other City policies and work rules. The main points are:

- The City provides network, communications systems, equipment and devices (”technology resources”) to carry out legitimate City business. By using the City's technology resources, an employee consents to disclosing the contents of any data files, information and communications created on, stored on, transmitted, received or exchanged via its network, communications systems, equipment or devices.
- There is no right to privacy in the use of City technology resources. By using the City's technology resources an employee consents to monitoring, and reviewing the use of those technology resources.
- Users of city technology resources are expected to act lawfully, ethically and professionally, and to exercise common sense. Actions that are embarrassing to explain to the public, City Administration, City Council or media should be avoided.
- Users who are granted access to critical data are responsible for its protection.
- Incidental use for personal needs is allowed as long as that activity does not interfere with City business or conflict with any City policy or work rule (see additional restrictions below).
- Use of technology in violation of this policy is subject to disciplinary action up to and including termination.

The following work rules apply to anyone accessing or using the City's technology resources for any reason:

Ownership of Data

The City owns all data stored on its network and systems (including e-mail, voicemail and internet usage logs) and reserves the right to inspect and monitor any and all such communications at any time. The City may conduct audits of employee accounts in order to ensure compliance with policies and requirements, to investigate suspicious activities that could be harmful to the organization, to assist departments in evaluating performance issues and concerns, and to identify productivity or related issues that need additional educational focus within the City. Internet and e-mail communications may be subject to public disclosure and the rules of discovery in the event of a lawsuit. The City's Internet connection and usage by individuals is subject to monitoring. There is no right to privacy in an employee's use of City technology resources.

Specific Prohibitions and Limitations:

Other prohibitions and restrictions of all uses of the City of Camas technology resources includes but is not limited to the following:

- Conducting a private business
- Political campaigning
- Accessing sites which promote exclusivity, hatred, or positions which are contrary to the City's policy of embracing cultural diversity
- Accessing inappropriate sites including adult content, online gambling, and dating services;
- Accessing sites that promote illegal activity, copyright violation, or activity that violates the City's ethical standards
- Using the internet to obtain or disseminate language or material which would normally be prohibited in the workplace
- Using encryption technology that has not been approved for use by the City
- The use of personally owned technology for conducting City business, where official City records are created but not maintained by the City
- Making unauthorized general message distributions to all users (using the ALL Mail Group)
- Installing any software that has not been approved by the City
- Sharing or storing unlicensed software or audio/video files
- Using security exploit tools (hacking tools) to attempt to elevate user privileges or obtain unauthorized resources or accessing sites that distribute computer security exploits (hacking sites)
- Excessive use of social networking sites for personal use during business or working hours;
- Streaming media for entertainment, downloading large files, during work hours that could affect the network
- The use or installation of unauthorized Instant Messaging, e.g. AIM, Yahoo Instant Messenger, Meebo, IRC, etc.; links and attachments
- Using unauthorized Peer to Peer Networking, e.g. E-Mule, Kazaa, Limewire, Warez, etc.
- The Use of "Soft" VOIP phones, e.g. Skype, Vonage, etc. unrelated to City business

Personal Use

Technology resources may be used for incidental personal needs as long as such use does not result in or subject the city to additional cost or liability, interfere with business, productivity or performance, pose additional risk to security, reliability or privacy, cause or tend to cause damage to the City's reputation or credibility, or conflict with the intent or requirements of any City policy or work rule. Incidental personal usage should generally conform to limits typically associated with brief personal phone calls. This document does not attempt to address every possible situation that may arise. Professional judgment, etiquette, and common sense should be exercised while using City technology resources for personal use. All data stored on City systems including but not limited to email, documents, and photos are subject to public disclosure requests and the property of the City. There is no right to privacy in an employee's personal use of City resources.

Use of an employee's personal devices (i.e., smart phones, tablets, etc.) should be limited to scheduled breaks or their lunch hour. The employee must still adhere to all City work rules and policies including those listed in the "**Prohibitions and Limitations"** section above, and all personal devices should use the City's **CityofCamas_PublicAccess** Wi-Fi unless authorized by Department Head and used for business-specific purposes.

Internet and Intranet Usage

Employees must abide by limitations listed in section "**Prohibitions and Limitations**" when using the Internet or Intranet. Usage should be focused on business-related tasks.

Use of the Internet, as with the use of all technology resources, must conform to all City policies and work rules. Employees may not use any City resources to access inappropriate web sites unless specific exemptions are granted as a requirement of work duties (e.g., police have the ability to access sites on criminal activity, weapons etc.).
Staff using City-owned equipment should always login and use the City's secured Wi-Fi **CityofCamas_Staff**.

The City recognizes that public Internet communications technologies are effective tools to promote community and government interaction and that employees could have legitimate reasons to participate in public communication via blogging, discussion forums, wikis, mashups, social networking, message boards, e-mail groups and other media that are now commonplace tools by which people share ideas and information. Department Heads or City Administration must approve the uses and tools described above.

Since activities on public Internet communication sites are electronically associated with City network addresses and accounts that can be easily traced back to the City of Camas, the following rules must be followed for participation on these interactive public Internet communication sites:

- When expressing staff's personal view, make it clear that it does not necessarily represent the views of the City of Camas. Opinions or views other than those reflective of City policy must contain the following disclaimer: "The content of this electronic communication does not necessarily reflect the official views of the elected officials or citizens of the City of Camas."
- Always protect the confidentiality, integrity, and availability of all critical information.
- Employees must not post any material that is obscene, defamatory, profane, libelous, threatening, harassing, abusive, hateful, or embarrassing to or of any other employee, person, and/or entity.
- Public Internet communications activity should contribute to staff's body of work as an employee of the City and must not interfere with or diminish productivity.

E-Mail Usage

E-mail content must be consistent with the same standards as expected in any other form of written (or verbal) communication occurring in a business setting where documents are subject to public disclosure. The City manages its e-mail in accordance with records retention policies and procedures as defined and identified by the City Clerk's Office.

When using City email in lieu of an employee's personal email for personal use, use must be infrequent, and employees must always abide by the "**Prohibitions and Limitations"** section of this policy.

Staff may access web-based personal email but should not download personal documents or attachments from these sites.

Users should be attentive to emails that have unusual or questionable subject lines to mitigate spam, phishing 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 or script born viruses in email attachments immediately report it to IT Staff or email **ITDsupport@cityofcamas.us**.

Security

The Information Technology Department (ITD) is responsible for monitoring and authorizing access to central computer systems and applications. Approved staff will be assigned unique user IDs and passwords for such access. Each user is responsible for establishing and maintaining a password that meets City requirements (Minimum 8 characters, upper/lower case, numbers and special characters). The City's unique network passwords must be changed every 90 days – unless otherwise authorized or approved by ITD Director, employee's Department Head or City Administrator.

The use of another user's account and password or the 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. Staff who discovers unauthorized use of their accounts must immediately report it to the ITD Director or Department Head.

The City 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 City financially; put 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, police investigation information, etc. The City will restrict access to critical information only to staff who have a legitimate business need-to-know. Anyone accessing critical information is responsible for keeping an inventory of critical information and ensuring that access to it is limited and secured.

Staff with access to critical information are responsible for its protection. Staff must take reasonable steps to ensure the safety of critical information including: avoid putting critical data on laptops; by encrypting data any time it is electronically transported outside the City network; not saving or transmitting critical data to a home or external computer; ensuring inadvertent viewing of information does not take place, and destroying or rendering the information unreadable when done with it. Staff should not transport critical City data on unencrypted devices such as thumb drives, CD's, or smart phones. The City has standards for encrypted USB drives that should be used for this purpose. Information about these standards should be requested from the ITD Support Staff at ITDsupport@cityofcamas.us or through the City's CRM system.

ITD representative approval is required prior to moving any and all physical media containing critical or sensitive data from secured areas.

Network Access and Usage

The Information Technology Department (ITD) must approve all connecting devices to the City's network. This includes personal PCs, network hubs and switches, printers, handhelds, scanners, remote connections, and wireless or wired devices. The use of personal routers and wireless access points on the City network is strictly prohibited.

The installation, removal, or altering of any software on City-owned equipment is prohibited without authorization from the ITD or employee's Department Head.

City-owned smart phones (Internet and/or e-mail capable cell phones) must meet and adhere to the current standards for those devices as established by ITD. Personally owned smart phones or devices may not be connected to the City's network without specific authorization by ITD or Department Head and should instead use the Guest Wi-Fi access for internet resources.

Exploiting or attempting to exploit any vulnerability in any application or network security is prohibited. Sharing of internal information with others that facilitates their exploitation of a vulnerability in any application or network security is also prohibited. It is also prohibited to knowingly propagate any kind of spyware, and/or denial of service attack or virus onto the City network or computers. Staff who encounter or observe vulnerability in any application or network security must immediately report it to the Department Head or ITD Support Staff at ITDsupport@cityofcamas.us.

Non-City staff (e.g. vendors, contractors) are required to have their personal devices that need to connect to the City's technology resources scanned by ITD for virus detection prior to connecting. If the PC or device is going to continue to be connected to the City's network it must be scanned a minimum of every 30 days. Representatives of the contracting departments are responsible for assisting their contractors to engage ITD to perform these services by entering a service request in the City's CRM system.

Disabling, altering, over-riding, or turning off any mechanism put in place for the protection of the network and workstation environments is strictly forbidden. This includes the installation of any software designed to circumvent security measures.

Because of band-width limitations inherent in any network system, use of the City's network to download non-business related information that are likely to impact systems or services is strictly prohibited. Examples include streaming video (i.e. movies), downloading large files like MP3 or MOV files, playing online games, etc. Business-related downloads of this nature should be done during low-impact network time intervals as defined by ITD support staff.

Transmission, distribution, or storage of any information or materials in violation of federal, state or municipal law is prohibited. Software that is copyrighted or licensed may not be shared or illegally distributed. Copyright violations are federal offenses that may result in civil and criminal penalties to employees and the City of Camas.

Users must manage their electronic documents in accordance with records retention policies and procedures as defined and identified by the City Clerk's Office. Documents past their retention schedules should be deleted from the network to save space and eliminate the need to backup unnecessary files. Electronic documents should never be stored in duplicate on the City's network servers.

Access to the City's network via VPN (Virtual Private Network) requires approval from staff's Manager, Department Head or City Administration and used only for City business purposes. VPN accounts will be audited quarterly. Accounts not actively being used will be deactivated or removed. Reactivation of intermittently used VPN accounts for vendor support purposes will be monitored by ISD staff. VPN users must have commercial up-to-date anti-virus software running on any connected devices.

At least annually, departments need to review, approve or de-activate network accounts and accounts created for their applications. ITD will assist as needed in doing these reviews.

Administration, Reporting and Violations/Discipline

Department Directors will designate specific employees who have access to technology resources. Department Directors or their designee share responsibility for monitoring appropriate implementation of these policies and requirements. Department Directors are responsible for determining any and all disciplinary actions that may stem from violations of these policies and requirements.

A virus checker will be running on computers that are connected to the Internet, to check downloaded files, e-mail and attachments. Files brought in from outside sources will be checked for viruses before installation on any city-owned hardware. If you receive a pop-up screen indicating the presence of a virus, immediately report the message to the ITD. Do not continue to download any attachments that the system indicates contains a virus.

Any employee who observes or suspects a violation of these policies and requirements, particularly those that relate to security of the city's network, systems, and data, should immediately report these concerns to their Department Director.

Violations of this policy are subject to disciplinary action up to and including termination.

City of Camas
WASHINGTON

Receipt and Acknowledgement
of the
Technology Resources Usage Policy and Work Rules

I hereby acknowledge that I have read and understand the Technology Resources Usage Policy and Work Rules of the City of Camas. I agree to abide by this policy and understand that use of technology resources and email is a privilege, not a right.

I understand that if I violate such rules, I may be subject to disciplinary action up to and including termination, as outlined in contract if represented.

____
Name (printed)

____
Signature

____
Date

This signed form must be returned to the Administrative Services Director within (3) days of receipt.