

# City of Redmond Technology Usage Policy

---

## Purpose

The intent of the *Technology Usage Policy* is to define the acceptable use of technology at the City of Redmond and to ensure that the City complies with all legally mandated requirements. It outlines the responsibilities of those who work for and on behalf of the City in contributing to the maintenance and protection of its information resources in a secure, stable and cost-effective manner. This policy is consistent with the intent and requirements of the City's work policies and rules.

## Policy Scope

The City of Redmond's *Technology Usage Policy* defines the oversight, use and protection of the City of Redmond's computing equipment, network, voice, electronic communications and data repositories. This includes the acquisition, access and use of all software, hardware and shared resources, whether connected to the network, configured off the network, or while in transit (mobile).

It applies to all those who work on behalf of the City of Redmond including, but not limited to, employees, contractors, consultants, temporaries, supplementals, volunteers and other workers including all personnel affiliated with third parties. This policy also applies to all equipment that is owned or leased by the City regardless of project and program funding sources.\*

**Acquisition of Technology Resources** - Information Services must evaluate and approve all software, hardware, removable devices and related maintenance and support contracts, whether the selected products or solution will be on the network or off; used by one or many people; and for all program and project funding sources.\* In addition, acquisition of technology resources should conform to existing purchasing policies and procedures as defined in the Finance Handbook. Most City-owned technology has a pre-determined lifecycle replacement period and must be surrendered for replacement on a 1:1 basis or retired, according to that schedule. Such technology may not be redeployed or otherwise put back into use without approval from Information Services.

## Access to the City's Technology Resources

- Human Resources must approve the setup of new user\* accounts.
- Users are responsible to establish and maintain passwords consistent with the City's standards.
- User accounts and ALL passwords may not be shared with anyone other than the named owner. Examples include co-workers, subordinates, business associates, household members, etc.
- The individual logged onto the City network must be present while the logon credentials are being used to access Network resources, or must ensure that the account is locked or logged off and not being used by others when not present.
- Information Services must approve connection of all devices using the City's infrastructure (i.e. Internet, network, wireless channels and telephone lines).
- Information Services must approve installation of all software, including shareware\*, freeware\* and software that is obtained for evaluation purposes.
- Direct peer-to-peer\* connections and modems are provided only in unique circumstances, requiring prior approval from Information Services.
- Connection or installation of personally-owned hardware or software with the City-provided infrastructure (i.e. network, Internet, fax lines, telephone lines, and other computers) is not allowed.
- All activity resulting from device\*, network or software application access is the responsibility of the person assigned the user account.

## Internet and Intranet Usage

- Use of the Internet should be consistent with City policies and work rules. Incidental personal use of City resources is allowed as defined in the paragraph [Incidental Personal Use](#). See examples of incidental use in [Appendix B](#). Visiting, referencing, downloading and/or storing materials that are inappropriate in a work environment is prohibited unless such activity is specifically related to your job. Examples include but are not limited to data from sexually explicit sites, and those associated with violence, hate crimes or illegal activities.
- Content and images posted on the City's Intranet, Internet FTP, Social Media sites or sent via Twitter should be consistent with the City's policies and practices, and should conform to professional standards in tone and format.

# City of Redmond Technology Usage Policy

---

- All information that is posted, copied or shared, either on the City's Intranet, servers and desktops or on the City's Internet or Social Media sites, must be done so in accordance with the laws that govern copyrighted materials including, but not limited to, photographs, magazines, books, copyrighted music, the installation of any copyrighted software for which the City or end user does not have an active license, or the installation of "pirated" software.
- Web usage that significantly impacts network bandwidth may be restricted. Individuals should utilize only the City's tools (such as the City-standard browser) and recommended best practices to manage their connections when viewing, downloading, sharing and printing information to ensure that these shared resources are not negatively impacted.
- The City's Intranet bulletin board will be used to disseminate information, employee news, programs and events that are pertinent to the employee base. The citywide (!\_City) e-mail distribution list should be used for critical and time-sensitive City business information only.
- Any attempt to misrepresent one's identity on the Internet (via newsgroups, chat rooms, blogs, etc.) is prohibited.

## E-mail Communications

- The City provides access to and support of its own e-mail system and web-related components. Use of any other e-mail system to conduct City-related correspondence is not advised, due to public record laws.
- E-mail communications will conform to the same professional standards as with written and verbal business correspondence. A professional tone should prevail and content will be consistent with and representative of the City's policies and practices.
- Any attempt to misrepresent one's identity via e-mail is prohibited.
- E-mail is considered part of the public record and is subject to disclosure under Washington State law. Managing individual e-mail storage and retention is the responsibility of each individual, consistent with the City's document and records-retention guidelines. Effort should be made to restrict unnecessary e-mail traffic, including minimizing the size of attachment files; and using network drives instead of large distribution lists to share file attachments with large groups.

## Intellectual Property, Privacy and Monitoring

There is no right to privacy in the course of using the City's technology resources, whether conducting City business or for incidental personal use. The City owns all data stored on its network and peripheral devices and reserves the right to inspect and monitor any and all such use at any time (examples include e-mail, voice-mail, Internet logs, computers, laptops, handhelds, etc.). The City may conduct requested audits in order to ensure compliance with its policies and requirements, to respond to public disclosure\* requests, investigate suspicious activities or security threats, or to fulfill legally mandated requirements (i.e. software license rules, Payment Card Industry (PCI\*) regulations, and the Health Insurance Portability and Accountability Act (HIPAA\*) requirements).

## Incidental Personal Use

The City's technology resources including e-mail and Internet web browser are City property and intended for use to conduct City business by its authorized employees, contractors, consultants, temporaries, supplementals, volunteers and other workers including all personnel affiliated with third parties; hereafter referred to as the user. Limited personal use is permitted as long as it does not result in a cost to the City, does not interfere with the responsibilities and fulfillment of job 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.

As noted previously, there is no right to privacy in the course of using the City's technology resources, whether for City business or incidental personal use.

## **Permissible Use**

This policy allows *minimal* personal e-mail under specific circumstances. Personal e-mail must conform to permissible use standards and may not be related to activities listed as prohibited uses. Apart from this, the rule does not sanction the use of City computers for unofficial purposes, e.g., writing letters, playing computer games, surfing the Internet, etc.. Downloading personal email to the City's system or attaching a personal email box is prohibited. See [Appendix B](#) for specific examples of permissible personal use.

# City of Redmond Technology Usage Policy

---

## **Prohibited Uses**

A *prohibited use* is any use related to the conduct of an outside business; a use for the purposes of supporting, promoting, or soliciting for any non-City sponsored outside organization or group; or religious activity, campaign or political use; commercial use; posting to or buying from online auction or sales sites; use to conduct illegal activities; any entertainment uses; and/or uses which result in the City being placed on electronic mailing lists related to prohibited uses. See [Appendix B](#) for specific examples of prohibited use.

## **Security, Storage and Protection**

Effective security requires the participation and support of every user in the organization. The City employs enterprise tools to manage, monitor and protect the organization from internal and external security threats and data loss. In addition to these measures, it is the responsibility of individuals to remain vigilant in their awareness and protection of the City's resources, including equipment and data they have access to and while in their possession. Specific due diligence requirements are outlined below:

- City devices and computer equipment must be logged out or "locked" when unattended.
- All users must log off of their pc and leave it powered on at the end of their shift to enable off-shift maintenance and security updates
- Intruding or attempting to intrude into any gap in system or network security is prohibited. Sharing of information with others that facilitates their unauthorized access to the City's data, network or devices, or their exploitation of a security gap is also prohibited.
- It is the responsibility of each individual to prevent unauthorized and indiscriminate access to "personal information" (see Definitions) that could pose the threat of identity theft, thus risking a person's privacy, financial security and other interests.
- As noted above, user accounts and passwords may not be shared. The individual logged onto the City network must be present while logon credentials are being used to access Network resources
- In general it is not permissible to download "personal information" to any removable/portable device, including laptop computers, unless access to that information is within the scope of your job, your manager has approved the copy of information to a portable device and the data or device is encrypted\*. Please see the City's Personal Information Security policy for further information.
- Removable devices\* such as USB drives and PDA/handhelds/smart phones, cameras, etc., must always be password-enabled.
- Transmitting confidential\* data in part or full via e-mail or other unencrypted medium is prohibited.
- Leaving personal, sensitive\* or confidential\* information exposed to view while unattended, either on paper or on screen, is prohibited.
- Whenever possible, laptop and desktop hard drives and removable devices should only contain *copies* of source files, not the original file.
- Individuals must report to the City any equipment, software or data that is lost, damaged or stolen at their first available opportunity. Reports will be made to a supervisor, manager or director. Unrecoverable equipment may incur additional replacement costs.
- Lost equipment, especially that containing sensitive or confidential information as defined here, must be reported immediately to the I.S. Support Line - 425-556-2929.
- Stolen computers, laptops, PDA's, thumb drives, etc. must be reported immediately (24 hours per day) to the I.S. Support Line 425-556-2929 and your local Police Department.
- Individuals must utilize City provided anti-virus software and scanning tools regularly to scan material from removable devices\* prior to use.
- Storage of any copyrighted material on a network server or local hard drive including, but not limited to, photographs from magazines, books or other copyrighted sources, copyrighted music, the installation of any copyrighted software for which the City or end user does not have an active license, or the installation of "pirated" software is strictly prohibited.

## **Reporting and Administration**

Anyone who observes or suspects a violation of these policies and requirements, or a potential gap in security or protection of the City's assets or data, should immediately report these to their department

## City of Redmond Technology Usage Policy

---

supervisor, manager or director, or the Human Resource Department. Violations may result in disciplinary action up to and including termination of employment. Requests for exceptions to any of the Technology Usage Policy definitions must be submitted in writing from department directors to Information Services. Exceptions require the approval of both the requesting department's director and Information Services' Manager. Approvals must be documented in writing and limited in duration to provide for periodic re-evaluation.

# City of Redmond Technology Usage Policy

## APPENDIX A DEFINITION OF TERMS

---

**CONFIDENTIAL (DATA)** - for purposes of this policy, examples include but are not limited to social security numbers, health and insurance information, and any combination of information that would allow a person's identity or information to be further compromised (credit card number and name).

**DEVICE** - any piece of equipment attached to a computer in order to expand its functionality. Some of the more common peripheral devices are printers, scanners, disk drives, tape drives, microphones, speakers, cameras, etc. For purposes of this policy, the word device also includes removable devices such as USB devices, cell phones, etc..

**ENCRYPTION** - a process by which data is converted into a form that cannot be easily understood by unauthorized access. It is generally thought that encryption is the final layer of data protection, since it assumes the device on which the data is stored has already been compromised. Unless the perpetrator has the encryption key, they cannot decode any of the data stored there. In the most secure environments, entire hard drives can be maintained in an encrypted state. This is typically only recommended on mobile devices, not those that are already secured inside an organization's network.

**FTP (File Transfer Protocol)** - a communications protocol that is used to connect two computers over the Internet so that the user of one computer can transfer files and perform file commands on the other computer. Companies will often create FTP sites to allow sharing of large files.

**FREEMWARE / SHAREWARE** - *Freeware* is copyrighted computer software which is made available for use free of charge, for an unlimited time. Google and Yahoo tools for personal use are an example of Freeware. Shareware generally requires the user to pay for software use after a designated trial period. The biggest issue with such programs is that there aren't any standards applied to its development; and thus there is little in the way of validation between legitimate and non-legitimate products. Recent industry studies have shown that even with legitimate programs, up to 76% of them are abandoned and never updated. Oftentimes the terms *shareware* and *freeware* are used loosely on non-legitimate Internet sites to entice unsuspecting end users to download files and programs that contain viruses or other malware. Items that are designated as Free for personal use may have licensing implication for Business use. Government use is considered business use.

**FUNDING SOURCE** - examples include but are not limited to: operational funds, the general fund, capital equipment project funding, grant-funded projects and programs, research and development funds and donations.

**HIPAA** - To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, included "Administrative Simplification" provisions including national standards for electronic health care transactions. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information, so also incorporated provisions that mandated the adoption of Federal privacy protections for individually identifiable health information. Any agency or entity that stores health-related data must conform to the provisions as outlined in HIPAA.

**PCI / DSS** - stands for Payment Card Industry Data Security Standard. This set of policies and processes was developed by the major credit card companies as a requirement to help organizations that process credit card payments to prevent fraud, hacking and various other security issues. A company processing credit card payments must be PCI compliant or they risk losing the ability to process credit card payments.

**PEER-TO-PEER** - A peer-to-peer (or P2P) computer network relies primarily on the computing power and bandwidth of the participants in the network rather than concentrating it in a relatively low number of servers. A pure peer-to-peer network does not have the notion of clients or servers, but only equal *peer* nodes that simultaneously function as both "clients" and "servers" to the other nodes on the network.

**PUBLIC DISCLOSURE** - As a local government agency in the state of Washington, the City of Redmond is required by law to follow specific guidelines in the management of its public records. These guidelines include adhering to retention schedules and the specific handling of public disclosure requests. They also include definitions of what is disclosable and what is not.

# City of Redmond Technology Usage Policy

## APPENDIX A DEFINITION OF TERMS

---

**REMOVABLE DEVICE** - any storage device that can be removed from a computer, laptop or network with or without administrative privileges to the device. Examples include but are not limited to: removable hard drives; ipods; cameras; memory cards; thumb drives (aka "flash" drives); hot-swappable CD/DVD drives, etc.

**SENSITIVE (DATA)** - for purposes of this policy, "sensitive" refers to examples of information that relates to a person's state of employment, including personnel matters, disciplinary actions, and employee appraisal documentation. A good rule of thumb is that sensitive information is intended only for the parties who are directly involved or impacted by it. It would not be freely shared with others unless specifically warranted by permission or legal mandates.

**SOCIAL MEDIA** - media designed to be disseminated through social interaction, created using highly accessible and scalable publishing techniques. Social media supports the human need for social interaction, using Internet- and web-based technologies to transform broadcast media monologues (one to many) into social media dialogues (many to many). It supports the democratization of knowledge and information, transforming people from content consumers into content producers. Social media can take many different forms, including Internet forums, weblogs, social blogs, wikis, podcasts, pictures, video, rating and bookmarking.

**TECHNOLOGY RESOURCES** - the physical and communication components that are necessary for hardware and software applications to perform in a diverse corporate environment. These include but are not limited to the servers, complex network of cabling, telecommunication and Internet devices, etc. The ability to leverage existing infrastructure or extend its use is often a primary consideration in any new project proposal involving a technology component.

**USERS** - examples include but are not limited to full and part-time employees; council members; contractors or consultants with network accounts and those granted access to the secure City network or extranets; supplemental, temporary or limited-term employees; interns and volunteers.

---

Reference [www.wikipedia.com](http://www.wikipedia.com) for some definitions

# City of Redmond Technology Usage Policy

## APPENDIX B

---

### Examples of permissible personal e-mail use

The following are examples of allowable computer uses, so long as the permissible use requirements are met:

1. User sends an e-mail communication home to make sure his or her children have arrived safely from school.
2. User receives a brief e-mail from his or her son or daughter, who is away at college, solely for the purpose of telling the parent he or she is coming home for the weekend.
3. User is flying to visit relative but flight plans have changed, and user is sending e-mail solely for the purpose of informing the relative of the new arrival time.

### Examples of permissible computer use

The following are examples of allowable computer use, so long as the permissible use requirements are met:

1. Uses the Internet to view City job announcements from the Human Resources Department.
2. Goes to the City Intranet page to learn about City Wellness Programs. This is allowable, since the program is a part of the City benefit package available to users.
3. Uses the Internet to investigate issues surrounding his commute. This could include viewing pages at Metro to learn about transit schedules, WSDOT to look at freeway traffic conditions, the Greater Redmond Transportation Management Association and RideshareOnline.com, the rideshare matching program. It could also include checking weather related sites, especially by bicycle and pedestrian commuters to determine if they will get caught in a rainstorm.
4. Uses City computer to take on-line job-related training courses pre-approved by supervisor or manager in lieu of attending a similar class off-site.
5. Uses City computer to read the newspaper during breaks.

### Examples of non-allowable computer use

The following are examples of computer uses that are not allowed. This list is not intended to be all-inclusive. Additionally, any use that is not expressly allowed is considered to be not allowable:

1. Uses the Internet to track his personal investment portfolio.
2. Uses City e-mail to solicit for non-City sponsored charity or fundraiser.
3. Uses Internet to do personal research such as comparison-shopping for automobiles.
4. Uses City e-mail to sell or give away personal items; e.g. baseball or theater tickets.
5. Download software to City computer from the Internet.
6. Uses Internet to access nude or sexually explicit materials (text, photographs, graphics, etc.) that are not related to their duties.

When using your City computer it is a good idea to ask yourself this question: Can I directly support a work purpose for this use? If the answer is yes, there should be no problem. Apart from Incidental Personnel Use, if the answer is no, don't do it.

If you have questions as to what constitutes City business, please ask your supervisor or manager. If you have questions about this policy, please contact the Information Services Manager or Human Resources.

City of Redmond Technology Usage Policy  
APPENDIX B

---

My signature below indicates that I have received a copy of the Technology Usage Policy and have read and understand my responsibilities as a user of the City's technology resources. I understand this policy is subject to change without notice and agree to abide by it and all subsequent changes. I also understand that violation of the policy may result in disciplinary action including termination.

Employee Signature \_\_\_\_\_ Date \_\_\_\_\_

Employee Name (print) \_\_\_\_\_ Dept. \_\_\_\_\_

Employee's Supervisor Name (print) \_\_\_\_\_

*Please return this signature page to:*

*Information Services  
Support  
3SFN*