Excerpted from City of Redmond Personnel Manual

11.200 Information Technology Usage

Purpose

The intent of the Information Technology Usage Policy is to define the appropriate and 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.

Policy Scope

The City of Redmond's Information 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, supplemental employees, volunteers, and other workers including all personnel affiliated with third parties, hereafter referred to as the user. 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

No technology resources including, but not limited to, software, hardware, cloud services, portable devices, removable devices, and related maintenance and support contracts, may be purchased or used in connection with City business without first obtaining authorization from the Technology and Information Services Department (TIS). An employee desiring to obtain a technological resource should first contact the Service Desk.

Access to Technology Resources

- Passwords: Users are responsible to establish and maintain passwords consistent with the City's standards. A user who forgets his or her password should contact the Service Desk from an internal city telephone for assistance, use the password reset tool available on the City's Intranet, or the password reset tool available online. User accounts and passwords represent your identity and should not be shared with anyone. This prohibition on sharing of passwords applies even in emergent situations. In the event access to a user account is necessary while an employee is away or otherwise unavailable, the Service Desk should be contacted.
- Logging off: Users should lock their computer by pressing the Windows and L key simultaneously or log off their computer whenever they leave their work station to prevent unauthorized activity. All users should log off of their computer and leave it powered on at the end of their shift to enable off-shift maintenance and security updates.
- Responsibility for access: All activity resulting from device, network, or software application access is the responsibility of the person assigned the user account.
- Personal hardware and devices: Personal hardware and devices should not be connected to the City's computers by any employee.
- Personal software: Personal software should not be installed on the City's computers by any employee.

Security of Technology Resources

Effective security requires the participation and support of every user in the organization. It is the responsibility of every user of City technology to remain vigilant in their awareness and protection of the City's technology resources. Specific due diligence requirements are outlined below:

- Intruding or attempting to intrude into any gap in system or network security is prohibited. Sharing of information with others that may facilitate their unauthorized access to the

City's data, network, or devices, or their exploitation of a security gap, is also prohibited.

- User accounts and passwords may not be shared.
- It is the responsibility of each user to prevent unauthorized access to personal, sensitive, or confidential information that could present a risk of identity theft, thus jeopardizing a person's privacy, financial security, or other interests.
- In general, it is not permissible to download personal, sensitive, or confidential information to any removable/portable device, including laptop computers, USB devices, or thumb drives unless access to that information is within the scope of your job, and the data or device is encrypted. Transmitting personal, sensitive, or confidential data in part or full via e-mail or other unencrypted medium is prohibited. Personal, sensitive, or confidential data should be stored in a file folder or SharePoint site that is accessible only to those who need to view it.
- Prior to accessing a removable device such as a USB or thumb drive, other mobile devices, cameras, etc., the user should scan for viruses and malware to avoid infecting the City's systems.
- 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. Original source files should be stored on the City's network or within SharePoint sites to ensure they are backed up to prevent loss.
- Lost or stolen computers, laptops, mobile devices, etc. must be reported immediately to the local Police Department. A report should also be made to a supervisor, manager, or director and to the TIS Service Desk at 425-556-2929 at the first available opportunity.
- Lost or stolen devices (including portable media such as thumb drives, CDs, DVDs) or hardcopy reports that contain personal, sensitive, or confidential information and/or information that is subject to Payment Card Industry Data Security Standards (pertaining to processing of credit card payments), the Health

Insurance Portability and Accountability Act (see Chapter 16 - HIPAA of this Manual), Criminal Justice Information Services Security Policy, or other legal mandate should be reported immediately to the TIS Service Desk at 425-556-2929 to determine any action that must be taken under those regulations.

Use of Technology Resources

The City's technology resources are City property and are intended to be used for the conduct of City business.

Use of City technology resources is not permitted when the use is related to the conduct of an outside business; is for the purpose of supporting, promoting, or soliciting for any non-City sponsored outside organization or group; religious, campaign or political use; commercial use; to conduct illegal activities; any entertainment use; use which results in the City being placed on electronic mailing lists related to prohibited uses; downloading personal email to the City's system or attaching a personal email box.

Limited personal use is permitted as long as the use does not result in a cost to the City, does not interfere with the user's 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. It is strongly advised that personal devices should be used to access the Internet or personal email while on breaks.

When using City technology 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. If the answer is no, you probably shouldn't do it unless you are confident that the use is permitted as a limited personal use described above. If you have questions about the appropriateness of using City technology resources for any particular purpose, contact the Technology and Information Services (TIS) Director or designee for guidance.

There is no right to privacy when using the City's technology resources, whether for City business or incidental personal use. The

City owns all data stored on its network and peripheral devices and reserves the right to inspect and monitor any use at any time (examples include e-mail, voicemail, internet logs, computers, laptops, mobile devices, etc.)

Internet and Intranet Usage

- Content and images posted on the City's intranet and Internet sites should conform to the same professional standards as with written business correspondence. A professional tone should prevail.
- All information that is posted, copied, or shared, either on the City's Intranet, servers, and desktops, the City's website or social media sites, should conform to laws that govern copyrighted materials including, but not limited to, photographs, magazines, books, music, or the installation of any software for which the City does not have an active license.
- The installation of pirated software is prohibited.
- 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.
- Any attempt to misrepresent one's identity on the Internet (via newsgroups, chat rooms, blogs, etc.) is prohibited.

Examples of Permissible Internet and Intranet Use

The following are examples of Internet/intranet use that will be allowed, so long as the previously stated permissible use requirements are met:

- Use of the Internet to view job announcements.
- Viewing the City intranet page to learn about City Wellness Programs.
- Use of the Internet to investigate issues surrounding an employee's commute. This could include viewing pages at

Metro to learn about transit schedules or WSDOT to look at freeway traffic conditions.
- Use of the Internet to check the weather for the upcoming weekend.
- Use of a City computer to do some comparative shopping during your break.

Examples of Impermissible Internet and Intranet Use

- Use of the Internet to access nude or sexually explicit materials (text, photographs, graphics, etc.) that are not related to the user's job duties.
- Supporting, promoting, or soliciting for any non-City sponsored outside organization or group.
- Conducting illegal activities.
- Engaging in activity that would violate the City's ethics and/or conflict of interest policies.

E-mail Use

- E-mail communications should conform to the same professional standards as with written business correspondence. A professional tone should prevail.
- Minimal personal use of the City's email system is permitted. However, personal e-mail must conform to limited use standards and may not be related to activities listed as prohibited uses.
- Use of e-mail systems other than the City's email system to conduct City business is not advised due to records retention and public disclosure laws.
- E-mail is considered a 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. Users should avoid unnecessary e-mail traffic and are encouraged to minimize the size of attachment files and use network drives or SharePoint sites to share file attachments.
- 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 when using City e-mail is prohibited.

Examples of Permissible E-mail Use

The following are examples of e-mail use that will be allowed, so long as the previously stated permissible use requirements are met.

- Sending an e-mail communication home to make sure one's children have arrived safely from school.
- Receiving an e-mail from a 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.
- When the user had planned to fly to visit relatives but flight plans have changed, and the user sends an e-mail solely for the purpose of informing the relative of the new arrival time.
- Use of City e-mail to solicit for a charity or fundraiser must be approved by the Mayor for City-wide distribution or department director for departmental distribution.

Examples of Impermissible E-mail Use

- Use of City e-mail to conduct illegal activities.
- Use of City e-mail to conduct an outside business.
- Engaging in activity that would violate the City's ethics and/or conflict of interest policies.
- Use of City email to campaign in support of or in opposition to a political candidate or ballot issue.

Text and Instant Message Use

- Text and instant messages should conform to the same professional standards as with written business correspondence. A professional tone should prevail.
- The use of text messaging and instant messaging to conduct City business from personal cell phones is prohibited. This prohibition applies even if the employee receives a stipend from the City to use the personal cell phone. The rationale behind this prohibition is that text messaging and instant

messaging on personal cell phones are not backed up on the City's server but, nevertheless, are government records subject to records retention laws and the Public Records Act, RCW 42.56.

- Text and instant messaging for conducting City business is permitted only on City equipment.
- Text and instant messaging should be used for transitory communication only.
- Any attempt to misrepresent one's identity when using City text or instant messaging is prohibited.

Examples of Permissible Text and Instant Message Use - City-Owned Devices Only

- "I'll be late to the meeting."
- "I'll meet you at 9:00."
- "Are you available for a quick chat?"

Examples of Impermissible Text and Instant Message Use

- "I authorize you to spend the $300,000 for that project."
- "City Council should authorize the ordinance pertaining to homelessness."
- Sending content (photo) that is subject to records retention laws instead of using email.

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 make a report to their department supervisor, a manager or director, or the Human Resource Department. Failure to do so may result in disciplinary action up to and including termination of employment.

Exceptions to this Information Technology Use Policy

Requests for exceptions to any provision of this *Technology Usage Policy* must be submitted in writing by a department director to the TIS Director. Exceptions require the approval of both the requesting department's director and the TIS Director.

Approvals must be documented in writing and limited in duration to provide for periodic re-evaluation.