

Please read through this policy.

TECHNOLOGY RESOURCE USAGE POLICY AND WORK RULES

Executive Summary

This policy is designed to establish acceptable and appropriate use of computer and information systems, networks and other information technology resources at the City of Bellevue. The purpose of these policies is to safeguard and protect all technology resources from anything other than authorized and intended use. The main points to remember are:

1. 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.
2. 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, recording, and reviewing the use of that technology resource.
3. Users are expected to act lawfully, ethically and professionally, and to exercise common sense. Actions that are embarrassing to explain to the public, City Council, City Manager or media should be avoided.
4. Users who are granted access to critical data are responsible for its protection.
5. 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.
6. Use of technology in violation of this policy is subject to disciplinary action up to and including termination.

(Technology definitions provided in section 12)

1. Scope

- 1.1. The following policies define appropriate use of the City of Bellevue network, computers, mobile computing devices, smart phones, all related peripherals, software, electronic communications, and Internet access. They apply to the access of the City's network and use of computing technology resources at any location, from any device, via wired or wireless connection. They apply to all users of City technology resources regardless of employment status. Access to all networks and related resources require that each user be familiar with these policies and associated work rules. The City of Bellevue authorizes the use of computing and network resources by City staff, contractors, volunteers and others to carry out legitimate City business. All users of City computing and network resources will do so in an ethical, legal, and responsible manner. All use of technology resources must be consistent with the intent and requirements of all City policies and work rules. Technology resources may not be used to facilitate operation of a personal business such as sale of cosmetics, consulting, etc.

2. Ownership of Data

- 2.1. The City owns all data, files, information, and communications created on, stored on, transmitted, received or exchanged via its network, communications systems, equipment and devices (including e-mail, voicemail, text messages and Internet usage logs even if such communications resides with a third party provider) and reserves the right to inspect and monitor any and all such communications at any time, for any

business purpose and with or without notice to the employee. The City may conduct random and requested audits of employee accounts (including accounts with commercial or other third party providers if used in the course of conducting City business) 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, e-mail, voicemail, text message communications and Internet usage logs may be subject to public disclosure and the rules of discovery in the event of a lawsuit. The City's Internet connection and usage is subject to monitoring at any time with or without notice to the employee. There is no right to privacy in the use of City technology resources.

3. Personal Use

- 3.1. 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 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. Please note that any data stored on City systems including but not limited to email, word documents, and photos may be subject to public disclosure requests.

4. Internet/Intranet Usage

- 4.1. This technology usage agreement outlines appropriate use of the Internet/Intranet. Usage should be focused on business-related tasks. Incidental personal use is allowed as discussed under this section, but there is no right to privacy in an employee's use of the Internet/Intranet. Employee Internet usage is monitored. Web Usage Reports are provided to Directors to help them monitor their staff's use of the Internet.
- 4.2. Use of the Internet, as with use of all technology resources, should conform to all City policies and work rules. Filtering software will be used by the City to preclude access to 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.). Attempts to alter or bypass filtering mechanisms are prohibited. When it is available BellevueConnectStaff should be used for wireless access. Staff using City equipment should not use BellevueConnect, BellevueConnectOutdoor or other outside wireless services to bypass web filtering and monitoring.
- 4.3. Except for City business related purposes, visiting or otherwise accessing the following types of sites is prohibited:
- "adult" or sexually-oriented web sites
 - sites associated with hate crimes or violence
 - personal dating sites
 - gambling sites
 - sites that would create discomfort to a reasonable person in the workplace

- 4.4. The City recognizes that public Internet communications technologies (Web 2.0) are effective tools to promote community and government interaction and that employees want 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.

However, 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 Bellevue, the following rules must be followed for participation on these interactive public Internet communication sites:

- a. When expressing staff's personal view, make it clear that it does not necessarily represent the views of the City of Bellevue. 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 Bellevue."
- b. Always protect the confidentiality, integrity, and availability of all critical information.
- c. 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.
- d. To protect staff's privacy and the privacy of others, phone numbers or email addresses must not be included in the content body.
- e. 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.

5. E-Mail Usage

- 5.1. 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.
- 5.2. Users must manage their e-mail in accordance with records retention policies and procedures as defined and identified by the City Clerk's Office.
- 5.3. Use of the "Everyone_COB" or "Everyone_Staff" distribution lists is restricted to the City Manager's Office, Department Directors and their specific designees. Under no circumstances should an employee "Reply to All" to an Everyone_COB or Everyone_Staff message.
- 5.4. External mass distribution e-mails to 50 or more recipients are prohibited from City e-mail accounts. Staff communicating to distribution lists of 50 or more recipients should utilize GovDelivery "E-Mail Alerts," (which allow people to sign up to receive e-mails whenever substantive changes are made to city web pages) or listserv technology.
- 5.5. The City provides staff access to and support of the Exchange/Outlook messaging (e-mail) system. Access or usage of any other messaging systems is not allowed unless it is web based. Subject to the personal use limitations explained above, staff may access web-based personal email but should not download personal documents or attachments from these sites. Staff may not install client based software such as AOL for internet service on city equipment.
- 5.6. 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 contact the support desk.

- 5.7. The use of e-mail to send or solicit the receipt of inappropriate content such as sexually oriented materials, hate mail, content that a reasonable person would view as obscene, harassing or threatening and having no legitimate or lawful purpose or contents falling within the inappropriate categories for internet usage is prohibited.
- 5.8. The incidental personal use of e-mail from a City account to express opinions or views other than those reflective of City policy must contain the following disclaimer: "The contents of this electronic mail message do not necessarily reflect the official views of the elected officials or citizens of the City of Bellevue."

6. **Security**

- 6.1. ITD must authorize all access to central computer systems. Each user is responsible for establishing and maintaining a password that meets City requirements as described in the City's [password policy](#). The use of another user's account or 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 IT Support at support@bellevuewa.gov or call x2886.
- 6.2. The City of Bellevue 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, banking information, police crime investigation information, etc.
- 6.3. 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; encrypting data any time it is electronically transported outside the City network; not storing, saving, or transmitting critical data to a home computer or other external computer; ensuring inadvertent viewing of information does not take place, and destroying or rendering the information unreadable when done with it.
- 6.4. Staff should not transport critical City data on unencrypted devices such as thumb drives, CD's, or Smartphones. The City has standards for encrypted USB drives that should be used for this purpose. Information about these standards can be obtained from ITD Support at support@bellevuewa.gov or call x2886.
- 6.5. Department ITGC representative approval is required prior to moving any and all physical media containing critical data (as defined in the City's [Data Classification Policy](#)) from a secured area.
- 6.6. The City will restrict access to critical information only to staff who have a legitimate business need-to-know. Each system owner is responsible for keeping an inventory of critical information and ensuring that access to it is limited.
- 6.7. Staff will be assigned unique user IDs and passwords for network access. Access to systems and applications containing critical information will only be allowed via unique user IDs. Access will be monitored and actions will be traceable to authorized users.

- 6.8. Staff are prohibited from sharing their passwords or allowing anyone else to use their network account for any reason.

7. Network Access and Usage

- 7.1. The Information Technology Department (ITD) must approve connecting devices to the City's network. This includes 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 not allowed.
- 7.2. The installation, removal, or altering of any software on City-owned equipment is prohibited without authorization from a department manager or designee.
- 7.3. 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 may be connected to the City's network after ITD approval. This approval will only be granted after verification that the phone meets City standards and staff have signed applicable smart phone and/or stipend agreements per the smart phone policy.
- 7.4. 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 IT Support at support@bellevuewa.gov or call x2886.
- 7.5. Staff must follow the privacy and rules governing the use of any information accessible through the network, even if that information is not securely protected.
- 7.6. Non-City staff (e.g. vendors, contractors) are required to have their personal computers (PC) scanned by ITD for virus detection prior to connecting to the City's network. If the PC is going to continue to be connected (even occasionally) 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 contacting ITD Support at support@bellevuewa.gov or calling x2886.
- 7.7. 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.
- 7.8. Because of band-width limitations inherent in any network system, use of the City's network to download non-business related information is prohibited. Examples include streaming video of baseball games, streaming audio of radio programs, MP3 files, on-line games, etc.
- 7.9. 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 Bellevue.
- 7.10. 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.

- 7.11. Access to the City's network via VPN requires approval from ITD. 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 accommodated upon request. VPN users must have commercial up-to-date anti-virus software. Vendors accessing the City network via VPN must adhere to the rules in the Vendor VPN Access SOP
- 7.12. Remote access to the City's applications via Citrix requires approval from the employee's manager or supervisor.
- 7.13. At least annually, departments need to review and approve network accounts and accounts for their applications. ITD will assist as needed in doing these reviews.

8. Administration, Reporting and Violations/Discipline

- 8.1. Each Department will designate specific employees who have the authority to authorize ITD to provide accounts and access to technology resources. Suspected violations or concerns should be reported to IT Support at support@bellevuewa.gov or by calling x2886.
- 8.2. ITD, the Departments, and HR share responsibilities in enforcing the Technology Resource Usage Policy (TRUP) as follows

9. ITD Responsibilities

- 9.1. ITD is responsible for recommending TRUP guidelines that are enforceable.
- 9.2. ITD is responsible for enterprise monitoring of technology resources using security and monitoring tools. Security and monitoring information will be provided to HR as requested to support the investigation of TRUP or other policy violations.
- 9.3. If, in the normal course of business activities, ITD discovers violations of the TRUP, ITD will report the activities to the employee's supervisor, Director of HR, and/or to the City Manager depending upon the severity of the infraction.

10. Departments Responsibilities

- 10.1. Departments assist in the development and adoption of the TRUP through ITGC.
- 10.2. If, in the course of normal business activities, department management suspects an employee has or is violating the TRUP they must report the suspected infractions to Human Resources.
- 10.3. Departments are responsible for carrying out any disciplinary actions in response to TRUP violations.
- 10.4. Assist in education and communication on an ongoing basis

11. Human Resources Responsibilities

- 11.1. Human Resources assists in the development and adoption of the TRUP through ITGC.
- 11.2. Human Resources is responsible for integrating the TRUP into new hire orientation and training and ongoing training of City work rules and policies.
- 11.3. Human Resources is responsible for the evaluation of reported TRUP infractions, and may request additional monitoring information (e.g., security logs) from ITD as part of their investigation and evaluation process
- 11.4. Human resources is responsible for providing necessary information to Department Directors to facilitate and coordinate with department management the consistent application of disciplinary action when TRUP infractions occur.

- 11.5. As with any set of policies or rules, exceptions may be granted and documented on a case-by-case basis. These require authorization from the Department involved as well as from ITD. Some exceptions may also require City Manager approval.
- 11.6. Violations of the TRUP, work rules, or otherwise inappropriate use of technology resources are subject to disciplinary action up to and including termination. Actions that demonstrate a clear disregard for these policies and requirements and either resulted or could have resulted in damage or serious disruption to the City's network, systems, services, or data; or either resulted or could have resulted in damage to the City's credibility or reputation with the public may result in immediate discharge.

12. Definitions: (Courtesy of WebOpida.com and Wikipedia.com)

- 12.1. Blog - Short for Web log, a Blog is a Web page that serves as a publicly accessible personal journal for an individual. Typically updated daily, blogs often reflect the personality of the author. Blogging is when one posts to a Blog.
- 12.2. Incidental use – The use of City systems for limited personal use such as Internet browsing to look for and order personal items. This use should be limited to personal time such as lunch and breaks.
- 12.3. Mashup - a Web page or application that uses and combines data, presentation or functionality from two or more sources to create new services.
- 12.4. Media – see Physical Media
- 12.5. Phishing - The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.
- 12.6. Physical Media – Media which is utilized to store data and could potentially be used to transport information out of secure areas. These include but are not limited to paper reports, faxes, thumb drives, and CDs.
- 12.7. Spyware - Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with Spyware. Once installed, the Spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.
- Spyware is similar to a Trojan horse in that users unwittingly install the product when they install something else. A common way to become a victim of Spyware is to download certain peer-to-peer file swapping products that are available today.
- 12.8. VPN – Short for virtual private network, a network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted. VPN is used by outside computers to connect to the City of Bellevue network.