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 used by City of Bellevue staff, contractors, volunteers and others to conduct City business. 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, devices and access to cloud services (”technology resources”) to carry out legitimate City business. By using these technology resources, any user 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, third party hosted applications, cloud services, equipment or devices.
2. There is no right to privacy in the use of City technology resources. By using the City’s technology resources any user 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 good judgment.
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.

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 data 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 professional manner. All use of technology resources must be consistent with the intent and requirements of all City policies and work rules. Technology resources shall not be used to facilitate operation of a personal business.

2. Ownership of Data

2.1. The City owns all City data, files, information, and communications created on, stored on, transmitted, received or exchanged via its network, communications systems, equipment and devices, such as e-mail, voicemail, text messages and Internet usage logs “digital records” even if such communications reside in the cloud. The City reserves the right to inspect and monitor any and all such communications at any time, including personal data stored on City systems, for any lawful purpose and with or without notice to the user. 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) for any lawful purpose including but not limited to ensuring 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. Digital records 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 use as long as such use does not result in or subject the City to additional cost or liability, interfere with business, expected user 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. This Policy does not attempt to address every possible situation that may arise. Good judgment, etiquette, and common sense should be exercised while using City technology resources. Please note that any data stored on City systems or in City-provided cloud services including but not limited to email, documents, and electronic media are subject to search and may be disclosed in response to public disclosure requests.

4. Internet/Intranet Usage

4.1. This technology usage policy outlines appropriate use of the Internet/Intranet. Usage should be focused on business-related tasks. Incidental personal use is allowed as discussed in section 3.1, 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 Assistant/Deputy Director 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 BellevueConnect_Staff should be used for wireless access. Staff using City equipment should not use BellevueConnect, BellevueConnect_Outdoor or other outside wireless services to bypass web filtering and monitoring.

4.3. Except for City business related purposes, visiting or otherwise accessing sites such as the following are prohibited:

- Adult Content
- Games
- Violence
- Personals and Dating
- Gambling
- Hacking

4.4. The City recognizes that public Internet communications technologies and social media are effective tools to promote community and government interaction and that employees may want or need to participate in public communication as part of their job responsibilities via blogging, discussion forums, wiki e-mail groups and other media that are now commonplace tools by which people share ideas and information. Please refer to the HRPPM Social Media policy located in Chapter 5 Section 9 – Workplace Policies, for further details.

5. Messaging System Usage

Messaging systems include Outlook Email, IM, SFB, chat and voice services.

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 messages 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 500 or more recipients are prohibited from City e-mail accounts. Staff communicating to distribution lists of 500 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 messaging systems described above. 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 for internet service on city equipment

5.6. The use of messaging systems 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, having no legitimate or lawful purpose, or contents falling within the inappropriate categories for internet usage is prohibited.

5.7. The incidental personal use of messaging systems 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. The Information Technology Department (ITD) must authorize all access to 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 and other mobile devices; 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 or non-City provided cloud provider; 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 mobile devices. 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 Operations Policy Team 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. If staff discover that they have access to critical or confidential information not necessary to perform their job they must report it to ITD. 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, writing down their network password, and must report to ITD immediately, and change their password, if they suspect it has been compromised.

6.9. Credit card information must never be sent or received via messaging systems and staff are prohibited from copying, moving or storing of credit/debit card holder information onto local hard drives and removable electronic media when accessing such data via remote-access technologies.

6.10. Staff must get ITD approval prior to storing critical or confidential information using any cloud storage provider.

7. Network Access and Usage

7.1. 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 and ITD.

7.3. Mobile devices 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 mobile device meets City standards and staff have signed applicable mobile device and/or stipend agreements per the mobile device policy.

7.4. ITD has access to location information for some City- mobile devices. This information is point of time only and will not typically be used to track employee movement or travel. This information will be used primarily to locate lost equipment. Upon request ITD will provide mobile device information to HR and/or Legal.

7.5. 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.

7.6. Non-City staff (e.g. vendors, contractors) are required to have their personal computers (PC) scanned by ITD for virus detection prior to physically 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 sporting events, 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 if it is available for the device they are connecting from. Vendors accessing the City network via VPN must adhere to the rules in the Vendor VPN Access SOP

7.12. 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.

7.13. All devices accessing City network must be running up to date antivirus software if it is available for the device they are connecting from.

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, Department Director, Director of HR, and/or to the City Manager depending upon the severity of the infraction.

9.4. ITD will provide information security awareness training as part of new employee orientation and will incorporate the TRUP into this training.

10. Departments Responsibilities

10.1. Departments assist in the development and adoption of the TRUP through the Operations Policy Team.

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 the Operations Policy Team.

11.2. 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

11.3. 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.

11.4. 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 and HR. Some exceptions may also require City Manager approval.

11.5. Violations of the TRUP, work rules, or otherwise inappropriate use of technology resources are subject to disciplinary action up to and including termination. Those actions include demonstrating 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.

\ \ \ \ \