16.00.250 TECHNOLOGY RESOURCE USAGE (CALEA 11.4.4)

NOTICE: There is no right to privacy in an employee's use of City technology resources.

This policy applies to members of the Bellevue Police Officers Guild and the Bellevue Police Managers Association only. Other bargaining units within the Police Department elected to abide by City of Bellevue IT policy at Technology Usage Policy.

The City owns all data stored on its network and systems (including email, and Internet usage logs) and reserves the right to inspect and monitor any and all such communications at any time to ensure compliance to this policy, with or without notice to the employee. The City may conduct random and requested audits of employee accounts 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 email 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 is subject to monitoring at any time with or without notice to the employee.

The following policy defines appropriate use of the City of Bellevue network, computers, mobile computing devices, smart phones, all related peripherals, software, electronic communications, and Internet access, regardless of the means used to access the system.

Employees violating this policy may be subject to disciplinary action up to and including termination in accordance with their collective bargaining agreement.

1. **Internet / Intranet Usage**

    1. This technology usage policy outlines appropriate use of the Internet/Intranet. Usage should be focused on business-related tasks. Personal use is allowed but there is no right to privacy in an employee's use of the Internet/Intranet. Personal use should be limited to personal break time.

    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 actively 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.

    3. Except for police related purposes, intentionally visiting or otherwise accessing the following types of sites is prohibited:

        a. Adult Content
        b. Games
        c. Violence
        d. Personals and Dating
        e. Gambling
        f. Hacking

4. Activities on Internet chat rooms, blogs and interactive website communication sites are electronically associated with City network addresses and accounts that can be easily traced back to the City of Bellevue. Comments made during the course of business use shall be reflective of Bellevue Police Department policy.

2. Messaging System Usage

Messaging systems include outlook Email, Instant Messaging, Skype for Business, chat and voice services

1. Email content is subject to public disclosure; therefore, email content should be written with this in mind.

2. Employees should try to check their email each workday and comply with IT capacity limits. Messages should be stored to an alternative location (F drive or back-up disk or appropriate case or personnel file). Ordinary business correspondence has a two-year retention period. If email relates to a specific case or personnel issue the email should be placed in the appropriate case or personnel file for retention. Personal email should not be retained in the City system.

3. Use of the "Everyone_COB" or "Everyone_Staff" distribution lists are restricted to the City Manager's Office, Department Directors and their specific designees. Under no circumstances should an employee intentionally "Reply to All" to an "Everyone_COB" or "Everyone_Staff" message.

4. The City provides staff access to and support of the Exchange/Outlook messaging (email) 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 open or download personal documents or attachments from these sites. Staff may not install client based software for internet service on city equipment.

5. 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 at support@bellevuewa.gov or by calling 425-452-2886

6. Except for police related purposes, the use of email to intentionally 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.

7. The incidental personal use of email 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."

3. User Accounts

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.

2. Password Policy- The unauthorized use of another person's account or attempt to capture other users' passwords is prohibited. The unauthorized use of your account should be immediately reported to your supervisor and to ITD Support at Support@Bellevuewa.gov or call 425-452-2886.

4. Network Access and Usage

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.

2. Use of wired or wireless modems on the City's network requires written approval from ITD. Approved devices with wired modems must be disconnected from the network prior to using the modem.

3. Personal software or devices may not be loaded or attached to any City-owned equipment without written authorization by a designated department manager and by ITD. The use of personal routers and wireless access points on the city network is not allowed.

4. Knowingly exploiting or attempting to exploit into any vulnerability in any application or network security is prohibited. Sharing of internal information to 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. If you encounter or observe vulnerability in any application or network security, report it to 425.452.2886 or Support@Bellevuewa.gov immediately.

5. Obey the privacy and rules governing the use of any information accessible through the network, even if that information is not securely protected.

6. Knowingly disabling, altering, over-riding, turning off any mechanism put in place for the protection of the network and workstation environments is strictly forbidden.

7. 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.

8. Because of bandwidth limitations inherent in any network system, use of the City network to download *non-business* related information is prohibited. Examples include streaming video of sporting events, streaming audio of radio programs, MP3 files, and on-line games.

9. Access to the City's network via VPN requires approval from ITD. VPN accounts will be audited on a quarterly basis, and accounts inactive for 30 days will be deactivated unless an exception is granted by ITD. Reactivation of intermittently used VPN accounts for vendor support purposes will be accommodated upon request.