12.110 – Use of Department E-Mail & Internet Systems

Effective Date: 08/01/2021

The Seattle Police Department provides email service and internet access to conduct department business.

The guidelines in this section are not exclusive. They provide a general framework of prohibited and acceptable email and internet use.

This section applies to all employees and their access to the internet while on city equipment or while on-duty and their use of city email by any means.

12.110-POL

1. The City of Seattle Owns the Email and Internet Systems and Determines Appropriateness

The city owns the computers, email, and internet access systems and may monitor email and internet use for policy compliance. The city retains the right to determine what is appropriate for the workplace.

Department supervisors ensure that their staff is familiar with and adhere to department and city email and internet policy.

2. The Department Allows Limited Personal Use of Email and Internet

Recognizing the realities of the workplace, the department allows limited personal use of email and the internet. Occasional personal use is permissible if it follows the policies and usage standards set by the department and the city.

3. Department Email and Internet Use is Subject to Public Disclosure

There is no expectation of privacy in using department email or internet services on department-owned computers. All use of department computers, whether official or personal, is subject to public disclosure laws and can be discoverable in a lawsuit.

This information includes, but is not limited to internet usage, email, and chat messages in meeting applications such as Webex, Teams, and Zoom.

4. All Email and Internet Communications Must be Professional, Appropriate, and Lawful

All email communications and internet use must comply with department and city policies on professionalism and harassment in the workplace.

All internet use on department computers must comply with all laws and policies. This includes policies on privacy issues, any release of confidential, sensitive, or classified information, or information exempt from public disclosure.

Employees will use email signatures consistent with the City of Seattle Brand Guidelines. Email signature templates and instructions are available in this document and on the city's Brand Portal on SharePoint.

5. Employees Will Not Send Criminal Justice Information (CJI) via Email Without Encryption

Employees may only send CJI via email by activating Office Message Encryption (OME).

To activate message encryption for an email, employees will include the trigger word "COSSecure" in the subject line of an email message sent from an SPD Outlook email account.

Employees may only send encrypted emails containing CJI to recipients that are members of a Criminal Justice Agency and allowed to receive CJI information.

Examples of common CJI Data include:

- WACIC/NCIC hits

- SID number

- FBI number

- DOL photos obtained via ACCESS (OMNIXX)

(See also manual section 12.050 - Criminal Justice Information Systems)

6. Employees Will Read Email At Least Once per Shift and Respond Appropriately

Employees are not required to read or respond to email when off-duty or during a system outage or technical failure that prevents the receipt or sending of email.

Employees will respond (when applicable) to High Importance emails within four business days, or sooner if required by the subject matter.

Emails classified as High Importance are marked with an orange exclamation point and include the following subjects:

- Command staff communications
- Directives
- Special Orders
- Training Digests
- All other emails that are job-related, time-sensitive, and mandatory for the recipient
- These include subpoenas, wanted bulletins, information bulletins, investigative follow-up requests, statement requests, pre-trial discovery requests, and seizure hearing notices.

7. Employees Will Activate Automatic Email Replies for Extended Absences

Employees will activate their email Automatic Replies (Out of Office) in Outlook when they expect that they will be unable to respond to email for a period that exceeds four business days.

8. External Emails Will Contain Employee Contact Information

All email correspondence going outside the department will include a signature file containing the employee's contact information, including email address, business address, and desk phone numbers.

If an employee is not assigned a desk phone number, the employee's signature file will contain the unit or precinct main phone number.

For officer and community safety and data security purposes, employees issued a department smartphone will not include that number in an email signature file.

9. General Distribution Emails Require Lieutenant Approval

Emails going to large distribution lists such as SPDALL or SPDSWORN are general distribution emails. These emails require approval from a lieutenant or above and must include the name of the approving employee in the email.

When sending a general distribution email, employees will enter the recipients using the "Bcc" (blind carbon copy) field. The "Bcc" field will prevent unnecessary disclosure of email addresses, reduce vulnerability to junk email, and improve the chances of the email being successfully sent. The "To" field is not designed to handle a large number of addresses.

10. Employees Must Use Caution When Opening Email Attachments

Employees may contact Seattle IT if they have questions about an email attachment. Due to the risk of computer virus attacks, employees should not open email attachments from an unknown source.

11. Section Captain or Director Approves "Send As" Privileges for Shared Email Accounts

Employees must request "Send As" privileges for a shared mailbox, and/or request that a shared mailbox be created, by submitting a request via email to their section captain or director.

Employees will forward the approval to Seattle IT and initiate a service request.

12. Employees Will Not use Department Email, Internet, Computers, Cell Phones or Electronic Devices to Conduct a Personal For-Profit Business

13. Employees Will Not use Department Email, Internet, Computers, Cell Phones or Electronic Devices to Review Personal Investments or to Transact any Investment Business

These types of transactions include trading in stocks, bonds, or mutual funds.

Exception: Employees may conduct infrequent, brief checks of their investments in the city's Deferred Compensation Program since this is a city-sponsored and city-maintained program.

14. Employees Will Not use Department Email, Internet, Computers, Cell Phones or Electronic Devices to Participate in any Campaign for Elected Office or for any Other Political Activity

This includes a prohibition on making any campaign contributions via a credit card and using a department computer to do so. Similarly, employees may not "lobby" elected officials through department computers.

15. Employees Will not use Department Email, Internet, Computers, Cell Phones or Electronic Devices to Engage in Demeaning or Defamatory Conduct

Examples of such prohibited activities include knowingly accessing pornographic materials or sites that promote exclusivity, hatred, or positions which are contrary to the city's policy of valuing cultural diversity.

Precincts and specialty units shall maintain a log to document access or attempts to access a website that contains sensitive content as described above. This log must be retained at the unit/precinct level for three years plus the current year.

If an employee accidentally accesses a website that contains pornographic, sexually explicit, inappropriate, or illegal materials, they must immediately leave the site and notify a supervisor. The information regarding the inadvertent access shall be recorded on the internet log maintained by the precinct or specialty unit as specified in section above.

The precinct or section captain or their designee will review the log annually for completeness.

The Audit, Policy, and Research Section will conduct an annual audit of the Offensive Material Internet Logs.

16. Employees Will Not Access Sites That Incur a Cost to the Department Without Prior Supervisor Approval

17. Employees Will Not Knowingly Access or Communicate any Material of an Obscene, Harassing, Discriminatory or Derogatory Nature

Examples of such material include sites or email containing racial or sexual slurs or jokes, or containing harassing, intimidating, abusive, or offensive material to or about others.

18. Certain Assignments May Require Access to Sensitive Sites

The department recognizes that certain employees, such as Human Trafficking and Investigation Support Unit detectives, may have a legitimate business purpose for accessing sites and information otherwise considered inappropriate or illegal.

If employees need to access such "sensitive sites," employees will abide by the following:

- Employees will obtain approval from an immediate supervisor before accessing sensitive sites. The supervisor will contact Seattle IT to request an exception to the web filtering protocols.

- Employees accessing such sites should exercise courtesy to others that may be present when doing so. This may include closing the door, turning the screen away, or notifying other employees beforehand.

19. Department Computer Usage is Subject to the Intelligence Ordinance

Employees will adhere to the following guidelines to avoid a violation of the investigation ordinance, SMC Chapter 14.12 ("Restricted information" is defined in SMC 14.12.030 (K)):

- Storage of "restricted information" (as defined in the ordinance) on disks or computer/network drives must comply with the ordinance.

- Employees may not create directories or subdirectories which organize/index "restricted information."

- Employees may not transmit "restricted information" including web addresses (URLs) to specific sites, via email.

- Employees may not create bookmarks or hotlists in web browsers which organize/index restricted information.